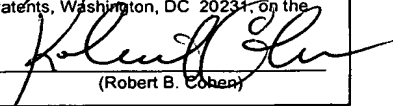


I hereby certify that this correspondence is being deposited with the U.S. Postal Service with sufficient postage as First Class Mail, in an envelope addressed to: Commissioner for Patents, Washington, DC 20231, on the date shown below.

Dated: April 24, 2002 Signature: 

(Robert B. Cohen)

Docket No.: SONYJP 3.0-238
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Tanaka, et al.

Application No.: 10/072,109

Filed: February 8, 2002

For: INFORMATION PROCESSING METHOD,
INFORMATION PROCESSING APPARATUS
AND RECORDING MEDIUM



Group Art Unit: 2131

Examiner: Not Yet Assigned

CLAIM FOR PRIORITY AND SUBMISSION OF DOCUMENTS

Commissioner for Patents
Washington, DC 20231

Dear Sir:

Applicant hereby claims priority under 35 U.S.C. 119 based on the following prior foreign applications filed in the following foreign countries on the dates indicated:

| Country | Application No. | Date |
|---------|-----------------|------------------|
| Japan | 2001-033114 | February 9, 2001 |
| Japan | 2001-094803 | March 29, 2001 |

In support of this claim, certified copies of the original foreign applications are filed herewith.

Dated: April 24, 2002

Respectfully submitted,

By 

Robert B. Cohen

Registration No.: 32,768

LERNER, DAVID, LITTENBERG,
KRUMHOLZ & MENTLIK, LLP

600 South Avenue West
Westfield, New Jersey 07090
(908) 654-5000
Attorneys for Applicant

502P0180US00

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年 2月 9日

出 願 番 号

Application Number:

特願2001-033114

[ST.10/C]:

[JP2001-033114]

出 願 人

Applicant(s):

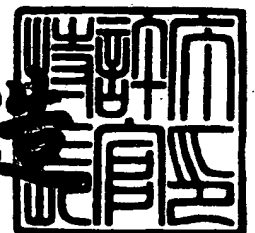
ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2002年 1月29日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



【書類名】 特許願

【整理番号】 0100063404

【提出日】 平成13年・2月 9日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/00

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
 内

 【氏名】 田中 浩一

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
 内

 【氏名】 河上 達

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
 内

 【氏名】 黒田 壽祐

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
 内

 【氏名】 石黒 隆二

【特許出願人】

 【識別番号】 000002185

 【氏名又は名称】 ソニー株式会社

【代理人】

 【識別番号】 100082131

 【弁理士】

 【氏名又は名称】 稲本 義雄

 【電話番号】 03-3369-6479

【手数料の表示】

【予納台帳番号】 032089

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9708842

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置および方法、プログラム格納媒体、並びにプログラム

【特許請求の範囲】

【請求項 1】 データの出力の指令を取り込む第 1 の取り込み手段と、
前記第 1 の取り込み手段が前記データの出力の指令を取り込んだ場合、暗号化した前記データを取り込む第 2 の取り込み手段と、
前記第 1 の取り込み手段が前記データの出力の指令を取り込んだ場合、前記データを利用するのに必要なライセンスを識別する識別情報を取り込む第 3 の取り込み手段と、
前記第 2 の取り込み手段により取り込まれた前記暗号化されたデータと、前記第 3 の取り込み手段により取り込まれた前記識別情報とを、所定のフォーマットにフォーマット化するフォーマット化手段と、
前記フォーマット化手段によりフォーマット化されたデータを出力する出力手段と

を備えることを特徴とする情報処理装置。

【請求項 2】 前記データを暗号化する暗号化手段を
さらに備えることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】 前記フォーマット化手段は、前記暗号化されたデータを復号するのに必要なキーをさらにフォーマット化することを特徴とする請求項 1 に記載の情報処理装置。

【請求項 4】 前記フォーマット化手段は、前記識別情報に対応する前記ライセンスを取得するためにアクセスするのに必要なアドレス情報をさらにフォーマット化する

ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 5】 前記ライセンスを保持する保持手段を
さらに備えることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 6】 前記識別情報に対応する前記ライセンスが前記保持手段に保持されているか否かを判定する判定手段と、

前記判定手段により前記ライセンスが前記保持手段に保持されていないと判定された場合、前記ライセンスを取得する取得手段を

さらに備えることを特徴とする請求項 5 に記載の情報処理装置。

【請求項 7】 前記ライセンスが有効であるか否かを判定する判定手段と、
前記判定手段により前記ライセンスが有効でないと判定された場合、前記ライセンスを更新する更新手段を

さらに備えることを特徴とする請求項 5 に記載の情報処理装置。

【請求項 8】 前記出力手段は、前記フォーマット化されたデータとともに、
前記保持手段により保持されている前記ライセンスも出力することを特徴とする請求項 5 に記載の情報処理装置。

【請求項 9】 前記暗号化されたデータを出力する経路がセキュアな経路であるか否かを判定する判定手段をさらに備え、

前記出力手段は、前記判定手段により前記暗号化されたデータを出力する経路がセキュアな経路であると判定されたとき、前記保持手段により保持されている前記ライセンスも出力する

ことを特徴とする請求項 8 に記載の情報処理装置。

【請求項 10】 前記ライセンスは、有効期間が異なる場合、異なる識別情報を有する

ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 11】 前記データはコンテンツデータであり、
前記ライセンスは、前記コンテンツをダウンロードすることができる有効期間、ジャンル、アーティスト、発売元、販売者、質、内容、または制作者に関する情報に基づいて規定される

ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 12】 前記データはコンテンツデータであり、
前記ライセンスは、前記コンテンツの利用の方法に基づいて規定されることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 13】 前記データはコンテンツデータであり、
前記ライセンスは、前記コンテンツの利用の回数に基づいて規定される

ことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 1 4】 データの出力の指令を取り込む第 1 の取り込みステップと

前記第 1 の取り込みステップの処理により前記データの出力の指令を取り込んだ場合、暗号化した前記データを取り込む第 2 の取り込みステップと、

前記第 1 の取り込みステップの処理により前記データの出力の指令を取り込んだ場合、前記データを利用するのに必要なライセンスを識別する識別情報を取り込む第 3 の取り込みステップと、

前記第 2 の取り込みステップの処理により取り込まれた前記暗号化されたデータと、前記第 3 の取り込みステップの処理により取り込まれた前記識別情報とを、所定のフォーマットにフォーマット化するフォーマット化ステップと、

前記フォーマット化ステップの処理によりフォーマット化されたデータを出力する出力ステップと

を含むことを特徴とする情報処理方法。

【請求項 1 5】 データの出力の指令を取り込む第 1 の取り込みステップと

前記第 1 の取り込みステップの処理により前記データの出力の指令を取り込んだ場合、暗号化した前記データを取り込む第 2 の取り込みステップと、

前記第 1 の取り込みステップの処理により前記データの出力の指令を取り込んだ場合、前記データを利用するのに必要なライセンスを識別する識別情報を取り込む第 3 の取り込みステップと、

前記第 2 の取り込みステップの処理により取り込まれた前記暗号化されたデータと、前記第 3 の取り込みステップの処理により取り込まれた前記識別情報とを、所定のフォーマットにフォーマット化するフォーマット化ステップと、

前記フォーマット化ステップの処理によりフォーマット化されたデータを出力する出力ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。

【請求項 1 6】 データの出力の指令を取り込む第 1 の取り込みステップと

前記第 1 の取り込みステップの処理により前記データの出力の指令を取り込んだ場合、暗号化した前記データを取り込む第 2 の取り込みステップと、

前記第 1 の取り込みステップの処理により前記データの出力の指令を取り込んだ場合、前記データを利用するのに必要なライセンスを識別する識別情報を取り込む第 3 の取り込みステップと、

前記第 2 の取り込みステップの処理により取り込まれた前記暗号化されたデータと、前記第 3 の取り込みステップの処理により取り込まれた前記識別情報とを、所定のフォーマットにフォーマット化するフォーマット化ステップと、

前記フォーマット化ステップの処理によりフォーマット化されたデータを出力する出力ステップと

をコンピュータに実行させるプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報処理装置および方法、プログラム格納媒体、並びにプログラムに関し、特に、著作権者からライセンスを受けていないコンテンツが不正にコピーされ、利用されるのを防止することができるようにした、情報処理装置および方法、プログラム格納媒体、並びにプログラムに関する。

【0002】

【従来の技術】

最近、インターネットを介して、ユーザが、自分自身が保持している音楽データを他のユーザに提供し、自分自身が保持していない音楽データを他のユーザから提供を受けるようにして、複数のユーザが無料で音楽データを交換しあうシステムが実現されている。

【0003】

このようなシステムでは、理論的には、1つの音楽、その他のコンテンツが存在すれば、他の全てのユーザが、それを利用することが可能となり、多くのユーザがコンテンツを購入しなくなるため、コンテンツに関する著作権者は、著作物

としてのコンテンツが売れないため、著作物の販売に伴い、本来受け取ることが可能な著作物の利用に関するロイヤリティを受け取る機会を失うことになる。

【0004】

【発明が解決しようとする課題】

そこで、コンテンツが不正にコピーされ、利用されることを防止することが、社会的に要請されている。

【0005】

本発明はこのような状況に鑑みてなされたものであり、コンテンツが不正に利用されるのを確実に防止することができるようにするものである。

【0006】

【課題を解決するための手段】

本発明の情報処理装置は、データの出力の指令を取り込む第1の取り込み手段と、第1の取り込み手段がデータの出力の指令を取り込んだ場合、暗号化したデータを取り込む第2の取り込み手段と、第1の取り込み手段がデータの出力の指令を取り込んだ場合、データを利用するのに必要なライセンスを識別する識別情報を取り込む第3の取り込み手段と、第2の取り込み手段により取り込まれた暗号化されたデータと、第3の取り込み手段により取り込まれた識別情報とを、所定のフォーマットにフォーマット化するフォーマット化手段と、フォーマット化手段によりフォーマット化されたデータを出力する出力手段とを備えることを特徴とする。

【0007】

前記データを暗号化する暗号化手段をさらに備えるようにすることができる。

【0008】

前記フォーマット化手段は、暗号化されたデータを復号するのに必要なキーをさらにフォーマット化するようにすることができる。

【0009】

前記フォーマット化手段は、識別情報に対応するライセンスを取得するためにアクセスするのに必要なアドレス情報をさらにフォーマット化するようにすることができる。

【0010】

前記ライセンスを保持する保持手段をさらに備えるようにすることができる。

【0011】

前記識別情報に対応するライセンスが保持手段に保持されているか否かを判定する判定手段と、判定手段によりライセンスが保持手段に保持されていないと判定された場合、ライセンスを取得する取得手段をさらに備えるようにすることができる。

【0012】

前記ライセンスが有効であるか否かを判定する判定手段と、判定手段によりライセンスが有効でないと判定された場合、ライセンスを更新する更新手段をさらに備えるようにすることができる。

【0013】

前記出力手段は、フォーマット化されたデータとともに、保持手段により保持されているライセンスも出力するようにすることができる。

【0014】

前記暗号化されたデータを出力する経路がセキュアな経路であるか否かを判定する判定手段をさらに備え、出力手段は、判定手段により暗号化されたデータを出力する経路がセキュアな経路であると判定されたとき、保持手段により保持されているライセンスも出力するようにすることができる。

【0015】

前記ライセンスは、有効期間が異なる場合、異なる識別情報を有するようにすることができる。

【0016】

前記データはコンテンツデータであり、ライセンスは、コンテンツをダウンロードすることができる有効期間、ジャンル、アーティスト、発売元、販売者、質、内容、または制作者に関する情報に基づいて規定されるようにすることができる。

【0017】

前記データはコンテンツデータであり、ライセンスは、コンテンツの利用の方

法に基づいて規定されるようにすることができる。

【0018】

前記データはコンテンツデータであり、ライセンスは、コンテンツの利用の回数に基づいて規定されるようにすることができる。

【0019】

本発明の情報処理方法は、データの出力の指令を取り込む第1の取り込みステップと、第1の取り込みステップの処理によりデータの出力の指令を取り込んだ場合、暗号化したデータを取り込む第2の取り込みステップと、第1の取り込みステップの処理によりデータの出力の指令を取り込んだ場合、データを利用するのに必要なライセンスを識別する識別情報を取り込む第3の取り込みステップと、第2の取り込みステップの処理により取り込まれた暗号化されたデータと、第3の取り込みステップの処理により取り込まれた識別情報とを、所定のフォーマットにフォーマット化するフォーマット化ステップと、フォーマット化ステップの処理によりフォーマット化されたデータを出力する出力ステップとを含むことを特徴とする。

【0020】

本発明のプログラム格納媒体のプログラムは、データの出力の指令を取り込む第1の取り込みステップと、第1の取り込みステップの処理によりデータの出力の指令を取り込んだ場合、暗号化したデータを取り込む第2の取り込みステップと、第1の取り込みステップの処理によりデータの出力の指令を取り込んだ場合、データを利用するのに必要なライセンスを識別する識別情報を取り込む第3の取り込みステップと、第2の取り込みステップの処理により取り込まれた暗号化されたデータと、第3の取り込みステップの処理により取り込まれた識別情報とを、所定のフォーマットにフォーマット化するフォーマット化ステップと、フォーマット化ステップの処理によりフォーマット化されたデータを出力する出力ステップとを含むことを特徴とする。

【0021】

本発明のプログラムは、データの出力の指令を取り込む第1の取り込みステップと、第1の取り込みステップの処理によりデータの出力の指令を取り込んだ場

合、暗号化したデータを取り込む第2の取り込みステップと、第1の取り込みステップの処理によりデータの出力の指令を取り込んだ場合、データを利用するのに必要なライセンスを識別する識別情報を取り込む第3の取り込みステップと、第2の取り込みステップの処理により取り込まれた暗号化されたデータと、第3の取り込みステップの処理により取り込まれた識別情報とを、所定のフォーマットにフォーマット化するフォーマット化ステップと、フォーマット化ステップの処理によりフォーマット化されたデータを出力する出力ステップとをコンピュータに実行させる。

【 0 0 2 2 】

本発明の情報処理装置および方法、プログラム格納媒体、並びにプログラムにおいては、暗号化されたデータと、そのデータを利用するのに必要なライセンスを識別する識別情報がフォーマット化され、出力される。

【 0 0 2 3 】

【発明の実施の形態】

図1は、本発明を適用したコンテンツ提供システムの構成を示している。インターネット2には、クライアント1-1, 1-2（以下、これらのクライアントを個々に区別する必要がない場合、単にクライアント1と称する）が接続されている。この例においては、クライアントが2台のみ示されているが、インターネット2には、任意の台数のクライアントが接続される。

【 0 0 2 4 】

また、インターネット2には、クライアント1に対してコンテンツを提供するコンテンツサーバ3、コンテンツサーバ3が提供するコンテンツを利用するのに必要なライセンスをクライアント1に対して付与するライセンスサーバ4、およびクライアント1がライセンスを受け取った場合に、そのクライアント1に対して課金処理を行う課金サーバ5が接続されている。

【 0 0 2 5 】

これらのコンテンツサーバ3、ライセンスサーバ4、および課金サーバ5も、任意の台数、インターネット2に接続される。

【 0 0 2 6 】

図2はクライアント1の構成を表している。

【0027】

図2において、CPU (Central Processing Unit) 21は、ROM (Read Only Memory) 22に記憶されているプログラム、または記憶部28からRAM (Random Access Memory) 23にロードされたプログラムに従って各種の処理を実行する。タイマ20は、計時動作を行い、時刻情報をCPU21に供給する。RAM23にはまた、CPU21が各種の処理を実行する上において必要なデータなども適宜記憶される。

【0028】

暗号化復号部24は、コンテンツデータを暗号化するとともに、既に暗号化されているコンテンツデータを復号する処理を行う。コーデック部25は、例えば、ATRAC (Adaptive Transform Acoustic Coding) 3方式などでコンテンツデータをエンコードし、入出力インタフェース32を介してドライブ30に接続されている半導体メモリ44に供給し、記録させる。あるいはまた、コーデック部25は、ドライブ30を介して半導体メモリ44より読み出した、エンコードされているデータをデコードする。

【0029】

半導体メモリ44は、例えば、メモリスティック (商標) などにより構成される。

【0030】

CPU21、ROM22、RAM23、暗号化復号部24、およびコーデック部25は、バス31を介して相互に接続されている。このバス31にはまた、入出力インタフェース32も接続されている。

【0031】

入出力インタフェース32には、キーボード、マウスなどよりなる入力部26、CRT、LCDなどよりなるディスプレイ、並びにスピーカなどよりなる出力部27、ハードディスクなどより構成される記憶部28、モデム、ターミナルアダプタなどより構成される通信部29が接続されている。通信部29は、インターネット2を介しての通信処理を行う。通信部29はまた、他のクライアントとの間で

、アナログ信号またはデジタル信号の通信処理を行う。

【0032】

入出力インタフェース32にはまた、必要に応じてドライブ30が接続され、磁気ディスク41、光ディスク42、光磁気ディスク43、或いは半導体メモリ44などが適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部28にインストールされる。

【0033】

なお、図示は省略するが、コンテンツサーバ3、ライセンスサーバ4、課金サーバ5も、図2に示したクライアント1と基本的に同様の構成を有するコンピュータにより構成される。

【0034】

次に、図3のフローチャートを参照して、クライアント1がコンテンツサーバ3からコンテンツの提供を受ける処理について説明する。

【0035】

ユーザが、入力部26を操作することでコンテンツサーバ3に対するアクセスを指令すると、CPU21は、通信部29を制御し、インターネット2を介してコンテンツサーバ3にアクセスさせる。ステップS2において、ユーザが、入力部26を操作して、提供を受けるコンテンツを指定すると、CPU21は、この指定情報を受け取り、通信部29から、インターネット2を介してコンテンツサーバ3に、指定されたコンテンツを通知する。図4のフローチャートを参照して後述するように、この通知を受けたコンテンツサーバ3は、暗号化されたコンテンツデータを送信してくるので、ステップS3において、CPU21は、通信部29を介して、このコンテンツデータを受信すると、ステップS4において、その暗号化されているコンテンツデータを記憶部28を構成するハードディスクに供給し、記憶させる。

【0036】

次に、図4のフローチャートを参照して、クライアント1の以上の処理に対応するコンテンツサーバ3のコンテンツ提供処理について説明する。なお、以下の説明において、図2のクライアント1の構成は、コンテンツサーバ3の構成とし

ても引用する。

【0037】

ステップS21において、コンテンツサーバ3のCPU21は、インターネット2から通信部29を介してクライアント1よりアクセスを受けるまで待機し、アクセスを受けたと判定したとき、ステップS22に進み、クライアント1から送信されてきたコンテンツを指定する情報を取り込む。このコンテンツを指定する情報は、クライアント1が、図3のステップS2において通知してきた情報である。

【0038】

ステップS23において、コンテンツサーバ3のCPU21は、記憶部28に記憶されているコンテンツデータの中から、ステップS22の処理で取り込まれた情報で指定されたコンテンツを読み出す。CPU21は、ステップS24において、記憶部28から読み出されたコンテンツデータを、暗号化復号部24に供給し、暗号化させる。

【0039】

記憶部28に記憶されているコンテンツデータは、コーデック部25により、既にATRAC3方式によりエンコードされているので、このエンコードされているコンテンツデータが暗号化されることになる。

【0040】

なお、もちろん、記憶部28に予め暗号化した状態でコンテンツデータを記憶させることができる。この場合には、ステップS24の処理は省略することが可能である。

【0041】

次に、ステップS25において、コンテンツサーバ3のCPU21は、暗号化したコンテンツデータを伝送するフォーマットを構成するヘッダに、暗号化されているコンテンツを復号するのに必要なキーと、コンテンツを利用するのに必要なライセンスを識別するためのライセンスIDを付加する。そして、ステップS26において、コンテンツサーバ3のCPU21は、ステップS24の処理で暗号化したコンテンツと、ステップS25の処理でキーとライセンスIDを付加したヘッダ

とをフォーマット化したデータを、通信部 29 から、インターネット 2 を介して、アクセスしてきたクライアント 1 に送信する。

【 0 0 4 2 】

図 5 は、このようにして、コンテンツサーバ 3 からクライアント 1 にコンテンツが供給される場合のフォーマットの構成を表している。同図に示されるように、このフォーマットは、ヘッダ (Header) とデータ (Data) とにより構成される。

【 0 0 4 3 】

ヘッダには、コンテンツ情報 (Content information)、デジタル権利管理情報 (DRM (Digital Right Management) information)、ライセンス ID (License ID)、イネーブリングキープブロック (EKB (Enabling Key Block)) および、EKB から生成されたキー K_{EKBK} により暗号化されたコンテンツキー K_c ($K_{EKBK}(K_c)$) が配置されている。

【 0 0 4 4 】

コンテンツ情報には、データとしてフォーマット化されているコンテンツデータを識別するための識別情報としてのコンテンツ ID (CID)、そのコンテンツのコーデックの方式などの情報が含まれている。

【 0 0 4 5 】

デジタル権利管理情報には、コンテンツを使用する規則および状態 (Usage rules/status) と、URL (Uniform Resource Locator) が配置されている。使用規則および状態には、例えば、コンテンツの再生回数、コピー回数などが記述される。

【 0 0 4 6 】

URL は、ライセンス ID で規定されるライセンスを取得するときアクセスするアドレス情報であり、図 1 のシステムの場合、具体的には、ライセンスを受けるために必要なライセンスサーバ 4 のアドレスである。ライセンス ID は、データとして記録されているコンテンツを利用するとき必要とされるライセンスを識別するものである。

【 0 0 4 7 】

データは、任意の数の暗号化ブロック (Encryption Ebnock) により構成される。各暗号化ブロックは、イニシャルベクトル (IV (Initial Vector))、シード (Seed)、およびコンテンツデータをキー $K'c$ で暗号化したデータ $E_{K'c}(data)$ により構成されている。

【0048】

キー $K'c$ は、次式により示されるように、コンテンツキー Kc と、乱数で設定される値 $Seed$ をハッシュ関数に適用して演算された値により構成される。

【0049】

$K'c = \text{Hash}(Kc, Seed)$

【0050】

イニシャルベクトル IV とシード $Seed$ は、各暗号化ブロック毎に異なる値に設定される。

【0051】

この暗号化は、コンテンツのデータを8バイト単位で区分して、8バイト毎に行われる。後段の8バイトの暗号化は、前段の8バイトの暗号化の結果を利用して行われるCBC (Cypher Block Chaning) モードで行われる。

【0052】

CBCモードの場合、最初の8バイトのコンテンツデータを暗号化するとき、その前段の8バイトの暗号化結果が存在しないため、最初の8バイトのコンテンツデータを暗号化するときは、イニシャルベクトル IV を初期値として暗号化が行われる。

【0053】

このCBCモードによる暗号化を行うことで、1つの暗号化ブロックが解読されたとしても、その影響が、他の暗号化ブロックにおよぶことが抑制される。

【0054】

なお、この暗号化については、図15と図16を参照にして、後に詳述する。

【0055】

以上のようにして、クライアント1は、コンテンツサーバ3からコンテンツを無料で、自由に取得することができる。

【0056】

しかしながら、各クライアント1は、取得したコンテンツを利用するとき、ライセンスを取得する必要がある。そこで、図6を参照して、クライアント1がコンテンツを再生する場合の処理について説明する。

【0057】

ステップS41において、クライアント1のCPU21は、ユーザが入力部26を操作することで指示したコンテンツの識別情報を取得する。この識別情報は、コンテンツのタイトルや、記憶されている各コンテンツ毎に付与されている番号などにより構成される。

【0058】

そして、CPU21は、コンテンツが指示されると、そのコンテンツに対応するライセンスIDを読み取る。このライセンスIDは、図5に示されるように、暗号化されているコンテンツデータのヘッダに記述されているものである。

【0059】

次に、ステップS42に進み、CPU21は、ステップS41で読み取られたライセンスIDに対応するライセンスが、クライアント1により既に取得され、記憶部28に記憶されているか否かを判定する。まだ、ライセンスが取得されていない場合には、ステップS43に進み、CPU21は、ライセンス取得処理を実行する。このライセンス取得処理の詳細は、図7のフローチャートを参照して後述する。

【0060】

ステップS42において、ライセンスが既に取得されていると判定された場合、または、ステップS43において、ライセンス取得処理が実行された結果、ライセンスが取得された場合、ステップS44に進み、CPU21は、取得されているライセンスは有効期限内のものであるか否かを判定する。ライセンスが有効期限内のものであるか否かは、ライセンスの内容として規定されている期限と、タイマ20により計時されている現在日時と比較することがで判断される。ライセンスの有効期限が既に満了していると判定された場合、CPU21は、ステップS45に進み、ライセンス更新処理を実行する。このライセンス更新処理の詳細は

、図8のフローチャートを参照して後述する。

【0061】

ステップS44において、ライセンスはまだ有効期限内であると判定された場合、または、ステップS45において、ライセンスが更新された場合、ステップS46に進み、CPU21は、暗号化されているコンテンツデータを記憶部28から読み出し、RAM23に格納させる。そして、ステップS47において、CPU21は、RAM23に記憶された暗号化ブロックのデータを、図5のデータに配置されている暗号化ブロック単位で、暗号化復号部24に供給し、復号させる。

【0062】

CPU21は、さらに、ステップS48において、暗号化復号部24により復号されたコンテンツデータをコーデック部25に供給し、デコードさせる。そして、コーデック部25によりデコードされたデータを、CPU21は、入出力インタフェース32から出力部27に供給し、D/A変換させ、スピーカから出力させる。

【0063】

次に、図7のフローチャートを参照して、図6のステップS43で行われるライセンス取得処理の詳細について説明する。

【0064】

最初にステップS61において、CPU21は、いま処理対象とされているライセンスIDに対応するURLを、図5に示すヘッダから取得する。上述したように、このURLは、やはりヘッダに記述されているライセンスIDに対応するライセンスを取得するときアクセスすべきアドレスである。そこで、ステップS62において、CPU21は、ステップS61で取得したURLにアクセスする。具体的には、通信部29を介してインターネット2からライセンスサーバ4にアクセスが行われる。このとき、ライセンスサーバ4は、クライアント1に対してユーザIDとパスワードの入力を要求してくる（後述する図9のステップS102）。CPU21は、この要求を出力部27の表示部に表示させる。ユーザは、この表示に基づいて、入力部26を操作して、ユーザIDとパスワードを入力する。なお、このユーザIDとパスワードは、クライアント1のユーザが、インターネット2を介してライ

センスサーバ4にアクセスし、事前を取得しておいたものである。

【0065】

CPU21は、ステップS63において、入力部26から入力されたユーザIDとパスワードを取り込むと、ステップS64において、通信部29を制御し、入力されたユーザIDとパスワードを、インターネット2を介してライセンスサーバ4に送信させる。

【0066】

ライセンスサーバ4は、図9を参照して後述するように、ユーザIDとパスワードに基づいてライセンスを送信してくる（ステップS107）か、または、条件が満たされない場合には、ライセンスを送信してこない（ステップS110）。

【0067】

ステップS65において、CPU21は、ライセンスサーバ4からライセンスが送信されてきたか否かを判定し、ライセンスが送信されてきた場合には、ステップS66に進み、そのライセンスを記憶部28に供給し、記憶させる。

【0068】

ステップS65において、ライセンスが送信されて来ないと判定した場合、CPU21は、ステップS67に進み、エラー処理を実行する。具体的には、CPU21は、コンテンツを利用するためのライセンスが得られないので、コンテンツの再生処理を禁止する。

【0069】

以上のようにして、各クライアント1は、コンテンツデータに付随しているライセンスIDに対応するライセンスを取得して、初めて、そのコンテンツを再生することが可能となる。

【0070】

なお、図7のライセンス取得処理は、各ユーザがコンテンツを取得する前に、予め行っておくようにすることも可能である。

【0071】

図8は、図6のステップS45におけるライセンス更新処理の詳細を表している。図8のステップS81乃至ステップS87の処理は、図7のステップS61

乃至ステップS67の処理と基本的に同様の処理である。ただし、ステップS83において、CPU21は、ユーザIDとパスワードだけでなく、ライセンスIDもユーザに入力させ、これを取り込む。そして、ステップS84において、CPU21は、ユーザIDとパスワードとともにライセンスIDを、ライセンスサーバ4に送信する。

【0072】

その結果、図9を参照して後述するように、ライセンスサーバ4は、更新したライセンスを送信してくるので、ステップS85において、CPU21は、更新されたライセンスが取得されたか否かを判定し、取得された場合には、ステップS86において、更新されたライセンスを記憶部28に記憶させる。何らかの理由により更新されたライセンスが取得できなかった場合には、ステップS87に進み、CPU21は、エラー処理を実行する。すなわち、このとき、ライセンスを更新することができなかったことになるので、ユーザのコンテンツの再生は禁止される。

【0073】

次に、図9のフローチャートを参照して、ライセンスサーバ4の処理について説明する。なお、この場合においても、図2のクライアント1の構成は、ライセンスサーバ4の構成としても引用される。

【0074】

ステップS101において、ライセンスサーバ4のCPU21は、クライアント1よりアクセスを受けるまで待機し、アクセスを受けたとき、ステップS102に進み、アクセスしてきたクライアント1に対して、ユーザIDとパスワード、並びに、ライセンスの更新処理の場合には、更新すべきライセンスのライセンスIDの送信を要求する。上述したようにして、クライアント1からユーザIDとパスワード、並びに必要なに応じてライセンスIDが送信されてきたとき、ライセンスサーバ4のCPU21は、通信部29を介してこれを受信し、取り込む処理を実行する。

【0075】

そして、ライセンスサーバ4のCPU21は、通信部29から課金サーバ5にア

クセスし、ユーザIDとパスワードに対応するユーザの与信処理を要求する。課金サーバ5は、インターネット2を介してライセンスサーバ4から与信処理の要求を受けると、そのユーザIDとパスワードに対応するユーザの過去の支払い履歴などを調査し、そのユーザが、過去にライセンスの対価の不払いの実績があるか否かなどを調べ、そのような実績がない場合には、ライセンスの付与を許容する与信結果を送信し、不払いの実績などがある場合には、ライセンス付与の不許可の与信結果を送信する。

【0076】

ステップS104において、ライセンスサーバ4のCPU21は、課金サーバ5からの与信結果が、ライセンスを付与することを許容する与信結果であるか否かを判定し、ライセンスの付与が許容されている場合には、ステップS105に進み、CPU21は、いま、クライアント1より要求されているのは、新たなライセンスの付与であるのか否かを判定する。すなわち、ステップS102において、クライアント1からユーザIDとパスワードとともに、ライセンスIDが取り込まれているか否かを判定する。ライセンスIDが取り込まれている場合には、新たなライセンスの付与の要求ではなく、既に与えられているライセンスの更新の要求であると判定し、ステップS106に進み、そのライセンスIDに対応するライセンスの有効期限を更新する。

【0077】

ステップS105において、新たなライセンスの付与の要求であると判定された場合（ライセンスIDが取り込まれていないと判定された場合）、またはステップS106において、ライセンス更新処理が完了した後、ステップS107に進み、ライセンスサーバ4のCPU21は、そのライセンス（新たなライセンスまたは更新したライセンス）を通信部29からインターネット2を介してクライアント1に送信させる。

【0078】

ステップS108においてライセンスサーバ4のCPU21は、ステップS107の処理で、いま送信したライセンスをステップS102の処理で取り込まれたユーザIDとパスワードに対応して、記憶部28に記憶させる。さらに、ステップ

S109において、CPU21は、課金処理を実行する。具体的には、CPU21は、通信部29から課金サーバ5に、そのユーザIDとパスワードに対応するユーザに対する課金処理を要求する。課金サーバ5は、この課金の要求に基づいて、そのユーザに対する課金処理を実行する。上述したように、この課金処理に対して、そのユーザが支払いを行わなかったような場合には、以後、そのユーザは、ライセンスの付与を要求したとしても、ライセンスを受けることができないことになる。

【0079】

すなわち、この場合には、課金サーバ5からライセンスの付与を不許可とする受信結果が送信されてくるので、ステップS104からステップS110に進み、CPU21は、エラー処理を実行する。具体的には、ライセンスサーバ4のCPU21は、通信部29を制御してアクセスしてきたクライアント1に対して、ライセンスを付与することができない旨のメッセージを出力し、処理を終了させる。

【0080】

この場合、上述したように、そのクライアント1はライセンスを受けることができないので、そのコンテンツを利用することができないことになる。

【0081】

以上の処理をまとめると、図10に示されるようになる。この例においては、ユーザは、クライアント1として、クライアント1-1A、1-1Bを有している。このユーザは、クライアント1-1Aに記憶したコンテンツデータを利用するとき、ユーザIDとパスワードを、ライセンスサーバ4に送信する。この例においては、ユーザIDは、'foobar'とされ、パスワードは、'xxx'とされている。ライセンスサーバ4は、そのユーザIDとパスワードに対応するユーザの受信処理を、課金サーバ5に要求する。課金サーバ5は、この受信要求に基づいて受信処理を行い、ライセンスの許可または不許可を表す受信結果を、ライセンスサーバ4に出力する。

【0082】

ライセンスサーバ4は、課金サーバ5からの受信結果に基づいて、それがライセンスを許可するものである場合には、クライアント1-1Aに対して、ライセ

ンスを送信する。

【0083】

このライセンスには、ライセンスIDの他、暗号化されているコンテンツデータを復号するのに必要なキー、ライセンスの有効情報 (Validity)、権限 (Capability)、および制限 (Limitations) が含まれている。

【0084】

ライセンス2に含まれるキーは、図5のEKBに含まれる、暗号化されているキー K_{EKBC} を復号するためのキーである。

【0085】

すなわち、図5に示すEKBには、コンテンツキー K_c を暗号化したキー K_{EKBC} が、キー K_{dnk} で暗号化された状態で含まれている。そこで、クライアント1は、ライセンスに含まれるキー K_{dnk} を用いて、EKBに含まれるキー K_{EKBC} を復号することができる。そして、そのキー K_{EKBC} を用いて、さらに、コンテンツキー K_c を復号することができる。

【0086】

有効情報には、そのライセンスが有効な期間が記述される。ライセンスは、この有効期間内においてのみ有効であり、そこに記述されている有効期間が経過した場合には、そのユーザは、もはや、そのコンテンツを使用する権限を有しないことになる (ライセンスを有しないことになる)。

【0087】

あるいはまた、この有効情報には、ダウンロード有効期間が記述される。このダウンロード有効期間は、そのコンテンツをコンテンツサーバ3からダウンロードすることが可能な期間を表している。ダウンロード有効期間内であれば、ユーザは、そのコンテンツをコンテンツサーバ3からダウンロードすることができる。一旦、ダウンロードしたコンテンツは、以後、永久に使用可能となる。この点、コンテンツに通常の有効期間が設定されている場合と異なる。

【0088】

これらのライセンスは、有効期間毎に、あるいはダウンロード有効期間毎に、複数用意される。換言すれば、有効期間あるいはダウンロード有効期間が異なる

場合、異なるライセンスが用意される。

【0089】

権限には、例えば、CD-Rに、コンテンツを書き込む権利や、ポータブルデバイスに、コンテンツをコピーする権利が記述される。

【0090】

制限には、コンテンツの利用回数を制限する値、あるいはコンテンツをダウンロードすることが可能な回数を制限する値などが記述される。

【0091】

さらに、ライセンスは、その内容に応じて異なるもの（異なるIDを有するライセンス）とされる。

【0092】

例えば、ライセンスは、コンテンツの作成有効期間毎に複数用意される。例えば、作成有効期間として、2001年12月31日が記述されている場合、そのライセンスを有するユーザは、2001年12月31日までに作成されたコンテンツを利用することが可能であり、2002年1月1日以降に作成されたコンテンツは利用することができないことになる。コンテンツの作成時期は、コンテンツの提供側において規定されるものであり、ユーザ側の事情において規定されるものではない。従って、クライアント1のタイマ20をユーザが不正に操作するなどにして、日時情報をずらしたとしても、不正な利用を防止することが可能となる。

【0093】

さらにライセンスは、クラシック、ポピュラーといったジャンル毎に複数用意したり、アーティスト毎に複数用意することもできる。また、ライセンスは、コンテンツの発売元会社毎に複数用意したり、コンテンツの販売店毎に複数用意することができる。これにより、ライセンスを発売元毎に、あるいは販売店毎に管理することが可能となる。

【0094】

また、ライセンスは、コンテンツの音質や画質といった質に対応して、複数用意することができる。これにより、例えば、コンテンツの質に応じてライセンス

の値段を変えるなどすることができる。

【0095】

ライセンスはさらに、エンドユーザが、例えばCDなどからコンテンツを作成することを許容したり、発売元自らが作成することを許容するものとしてすることができる。

【0096】

また、ライセンスは、アルバム1曲だけ、ライナーノート付、ジャケット写真付などの内容毎に、複数用意することができる。

【0097】

さらに、1つのライセンスにより、複数のコンテンツを利用できるようにすることができる。

【0098】

図3のフローチャートに示すように、コンテンツ自体は、コンテンツサーバ3から、各クライアント1が自由に提供を受けることができるようにすることで、コンテンツサーバ3側から、各クライアント1に対してライセンスの購入や特定サービスへの参加を促すメッセージを送信することができる。

【0099】

ライセンスの一部として提供するキーを、ユーザ毎に個別に用意することにより、不正な使用を抑制したり、排除することが可能となる。

【0100】

ユーザは、上述した場合と同様に、自分自身が有するクライアント1-1Bに対しても、自分自身が有する同一のユーザIDとパスワードを基に、必要なライセンスを受けることができる。

【0101】

次に、図11のフローチャートを参照して、クライアント1が記憶部28に記憶した、暗号化されているコンテンツデータを、他の記憶媒体にコピーする場合の処理について説明する。ユーザが、例えば、入力部26を構成するマウスを利用して、コピー元の記録媒体から、コピー先の記録媒体に、コピーするファイルをドラッグアンドドロップすることでコピーを指令すると、CPU21は、ステッ

プ S 1 2 1 において、指定されたコンテンツに関する情報を取り込む。そして、ステップ S 1 2 2 において、CPU 2 1 は、ステップ S 1 2 1 で取り込まれた情報に基づき指定されたコンテンツのデータを記憶部 2 8 から読み出す。

【 0 1 0 2 】

ステップ S 1 2 3 において、CPU 2 1 は、そのコンテンツの利用回数（いまの場合、コピー回数）が制限内であるか否かを判定する。すなわち、CPU 2 1 は、コピー回数に制限が設けられている場合、後述するように、ステップ S 1 3 0 においてコピーした回数をカウントし、記憶部 2 8 に記憶させている（図 5 の使用規則および状態に記述される）。CPU 2 1 は、その記憶されている回数とライセンスの内容として記述されている利用回数とを比較し、そのコピー回数がまだ制限値（ライセンス値）に達していない場合には、ステップ S 1 2 4 に進み、記憶部 2 8 に記憶されているコンテンツデータが暗号化されていない場合には、これを暗号化復号部 2 4 に供給し、暗号化させる。既にコンテンツデータが暗号化されている場合には、ステップ S 1 2 4 の処理はスルーされる。

【 0 1 0 3 】

ステップ S 1 2 5 において、CPU 2 1 は、コンテンツデータをコピーするとき出力するフォーマットのヘッダに、復号に必要なキーとライセンス ID を付加する。ステップ S 1 2 6 において、CPU 2 1 は、ステップ S 1 2 1 の処理で取り込まれた情報に基づき、コピー先は、クライアント 1 とセキュアな経路で接続されているデバイスであるか否かを判定する。コピー先が、セキュアな経路で接続されているデバイスである場合には、ステップ S 1 2 7 に進み、CPU 2 1 は、暗号化したコンテンツにヘッダを付加し、ライセンスとともにコピー先に出力する。これにより、図 5 に示されるようなフォーマットで、コンテンツデータがコピー先に出力され、コピーされるとともに、そのデータには、ライセンスそのものが付随して出力され、コピーされる。

【 0 1 0 4 】

ステップ S 1 2 6 において、コピー先は、クライアント 1 とセキュアな経路で接続されたデバイスでないと判定された場合、ステップ S 1 2 8 に進み、CPU 2 1 は、暗号化したコンテンツにヘッダを付加し、コピー先に出力する。すなわち

、この場合には、コピー先が著作権を管理する機能を有していないデバイスであるか、著作権を管理する機能を有していない装置により再生可能なデバイスであるので、ライセンスそのものは出力されない。

【0105】

その後、ステップS129に進み、CPU21は、コピー回数をカウントする必要があるか否かを判定する。すなわち、そのコンテンツは、ライセンスによりコピー回数が制限されているか否かを判定する。コピー回数が制限されている場合には、ステップS130に進み、CPU21は、そのライセンスに対応するコンテンツのコピー回数を1だけインクリメントして、記憶部28（図5の使用規則および状態）に記憶させる。ステップS129において、コピー回数をカウントする必要がないと判定された場合、ステップS130の処理はスキップされる。

【0106】

以上のようにして、コピー回数がインクリメントされると、コピー回数を何回か繰り返すうちに、ステップS123において、コピー回数が制限内ではないと判定されることになる。この場合、ステップS131に進み、CPU21は、エラー処理を実行する。すなわち、このとき、CPU21は、コピー処理を禁止させる。

【0107】

このようにして、著作権を管理する機能を有するコピー先に対しては、ライセンスとともに暗号化されたコンテンツデータがコピーされる。これに対して、コピー先がセキュアなデバイスでない場合（著作権を管理する機能を有していないデバイスである場合）には、ライセンスはコピーされない。従って、コピー先は、コピーしたデータを不正に（ライセンスを受けずに）利用することができず、不正な利用を抑制することができる。ライセンスを有するクライアントは、そのコピーされたコンテンツを利用することができる。

【0108】

図12は、以上の関係を模式的に表している。クライアント1-11Aは、インターネット2を介して、コンテンツサーバ3から暗号化されたコンテンツの提供を受け、記憶することができる。このコンテンツの伝送経路は、通常の経路で

あり、セキュアな経路ではない。すなわち、著作権管理が行われるような経路ではなく、誰でもが自由にコンテンツデータを取得することができる。

【 0 1 0 9 】

さらに、クライアント 1-11A は、ライセンスサーバ 4 から記憶したコンテンツを利用するライセンスをセキュアな経路で取得する。セキュアな経路であるから、誰でもが、このライセンスを取得できるわけではない。上述した例では、ユーザ ID とパスワードを、ライセンスサーバ 4 に送信し、ライセンスサーバ 4 が、課金サーバ 5 に対して与信を行うことで、セキュアな経路が実現されている。このようにして、クライアント 1-11A は、暗号化されたコンテンツとライセンスを記憶し、コンテンツを利用することができる。

【 0 1 1 0 】

図 12 の例では同様に、クライアント 1-13 も、コンテンツと、それを利用するライセンスを取り込み、利用している。

【 0 1 1 1 】

クライアント 1-11A は、ポータブルデバイス (PD) 1-11B に対して、セキュアな経路でコンテンツデータをチェックイン (Ci) したり、チェックアウト (Co) する機能を有している。そこで、この場合、クライアント 1-11B には、本方式における暗号化が解除された状態で (セキュアな系を確保するのに必要な暗号化は施されている)、すなわち、ライセンスを必要としない状態で、コンテンツデータが転送され、保持される。従って、ユーザは、このクライアント 1-11B を利用して、コンテンツを再生することができる。

【 0 1 1 2 】

さらに、クライアント 1-11A は、例えば、半導体メモリなどよりなるクライアント 1-11C に対して、通常の経路で暗号化されたコンテンツデータを転送し、記憶させることができる。ただし、ライセンスはセキュアな経路でクライアント 1-11C に転送される。クライアント 1-11C は、暗号化されたコンテンツだけでなく、ライセンスも記憶しているので、このクライアント 1-11C を、所定の他のクライアントに装着すれば、その装置でコンテンツを再生することが可能となる。

【0113】

ただし、この例では、クライアント1-12は、クライアント1-11Aから通常の経路で暗号化されたコンテンツの提供を受け、保持しているが、ライセンスを受けていないので、そのコンテンツを利用することができない。

【0114】

図13に示す例では、ユーザAのクライアント1-21は、ライセンスサーバ4からライセンスを受けており、ユーザBのクライアント1-22も、ライセンスサーバ4からライセンスを受けているので、ユーザBは、ユーザAのクライアント1-21からコンテンツデータをコピーしたとき、クライアント1-22で、そのコンテンツデータを利用することができる。

【0115】

これに対して、ユーザCのクライアント1-23は、ライセンスを受けていない。従って、ユーザAからコンテンツのコピーを受け取ったとしても、ユーザCのクライアント1-23は、それを利用することができない。

【0116】

もちろん、ユーザAのクライアント1-21は、コンテンツサーバ3から提供を受けたコンテンツを利用することができる。

【0117】

以上のように、本システムでは、暗号化されたコンテンツデータのコピーは自由であるが、それを再生したり、コピーしたりして、利用するとき、ライセンスが必要とされる。

【0118】

図14は、ライセンスの例を表している。この例においては、5個のコンテンツContent1乃至Content5が、1つのライセンスLicense1の対象とされている。そして、Content1乃至Content3は、それぞれContent Key1乃至Content Key3により暗号化され、これらのContent Key1乃至Content Key3は、それぞれ1つの暗号化キーであるLic.Key1により、さらに暗号化されている。

【0119】

また、Content4とContent5は、それぞれContent Key4とContent Key5によ

り、それぞれ暗号化され、Content Key4 とContent Key5 は、それぞれ1つの暗号化キーLic.Key2により、暗号化されている。

【0120】

図15は、ブロードキャストインクリプション (Broadcast Encryption) を、キーの管理方式に採用した場合におけるキーの構成方法を表している。図15に示されるように、キーは、階層ツリー構造とされ、最下段のリーフ (leaf) が個々のデバイス (図14の例ではコンテンツ) に対応する。図15の例の場合、番号0から番号15までの16個のデバイス (コンテンツ) に対応するキーが生成される。

【0121】

各キーは、図中丸印で示される各ノードに対応して規定される。この例では、最上段のルートノードに対応してキーKRが、2番目のノードに対応してキーK0、K1が、3段目のノードに対応してキーK00乃至K11が、第4番目のノードに対応してキーK000乃至キーK111が、それぞれ対応されている。そして、最下段のノードとしてのリーフ (デバイスノード) に、キーK0000乃至K1111が、それぞれ対応されている。

【0122】

階層構造とされているため、例えば、キーK0010とキー0011の上位のキーは、K001とされ、キーK000とキーK001の上位のキーは、K00とされている。以下同様に、キーK00とキーK01の上位のキーは、K0とされ、キーK0とキーK1の上位のキーは、KRとされている。

【0123】

コンテンツを利用するキーは、最下段のデバイスノード (リーフ) から、最上段のルートノードまでの1つのパスの各ノードに対応するキーで構成される。例えば、番号3のコンテンツを利用するキーは、キーK0011、K001、K00、K0、KRを含むパスの各キーで構成される。

【0124】

本発明のシステムにおいては、例えば、図16に示されるように、 $8 \times 24 \times 32$ 段のノードに対応するキーで構成されるMG-Rエンティティというキーシステ

ムが利用される。このキーシステムでは、ルートノードから下位の 8 段までの各ノードに対応するキーが、カテゴリが対応される。ここにおけるカテゴリとは、例えばメモリスティックなどの半導体メモリを使用する機器のカテゴリ、デジタル放送を受信する機器のカテゴリといったカテゴリを意味する。図 1 6 の例では、ルートノードから 8 段目のノードのうちの 1 つのノードに、本発明のシステムとしての T システムが対応される。この T システムのノードよりさらに下の階層の 2 4 段のノードに対応するキーにより、ライセンスが対応される。これにより、約 1 6 メガ ($= 2^{24} = \text{約 } 160 \text{ 万}$) のライセンスを規定することができる。さらに、最も下側の 3 2 段の階層により、約 4 ギガ ($= 2^{32} = \text{約 } 40 \text{ 億}$) のユーザを規定することができる。最下段の 3 2 段のノードに対応するキーが、DNK (Device Node Key) を構成する。

【 0 1 2 5 】

各コンテンツは、6 4 ($= 8 + 24 + 32$) 段の各ノードで構成されるパスの内の 1 つに対応される。すなわち、各コンテンツの暗号化には、割り当てられたパスを構成するノードに対応するキーが用いられる。上位の階層のキーは、その直近の下位の階層のキーを用いて暗号化され、図 5 の E K B 内に配置される。最下段の DNK は、E K B 内には配置されず、ライセンスに記述され、図 1 0 に示されるように、ユーザのクライアント 1 に与えられる。クライアント 1 は、ライセンスに記述されている DNK を用いて、コンテンツデータとともに配布される E K B 内に記述されている直近の上位の階層のキーを復号し、復号して得たキーを用いて、E K B 内に記述されているさらにその上の階層のキーを復号する。以上の処理を順次行うことで、クライアント 1 は、そのコンテンツのパスに属するすべてのキーを得ることができる。

【 0 1 2 6 】

例えば、図 5 の Data に、図 1 4 の Content 1 が格納されている場合、図 5 のコンテンツキー K_c は、Content Key 1 となり、キー K_{EKBC} は、Lic.Key 1 となる。この場合における図 5 の E K B は、図 1 7 に示されるように、 $K_{dnk}(\text{Lic.Key } 1)$ とされる。

【 0 1 2 7 】

図 1 7 において、K 1 (K 2) は、キー K 2 をキー K 1 で暗号化することを表している。

【 0 1 2 8 】

図 1 7 のキー Kdnk は、図 1 6 における DNK を意味し、このキー Kdnk が、図 1 0 に示されるように、ライセンスに含めてライセンスサーバ 4 からクライアント 1 に送信される。

【 0 1 2 9 】

クライアント 1 は、このキー Kdnk をライセンスを受けることにより得ることができるので、このキー Kdnk を用いて、EKB 中のキー Lic.Key 1 を復号し、この Lic.Key 1 を用いてキー Content Key 1 を復号する。さらに、クライアント 1 は、コンテンツキー Content Key 1 を用いて、Content 1 を復号する。

【 0 1 3 0 】

なお、本発明におけるキーは、図 1 5 および図 1 6 に示されるようなブロードキャストインクリプションを利用したキーシステム以外のキーで構成することも可能である。

【 0 1 3 1 】

また、本発明が適用されるクライアントは、いわゆるパーソナルコンピュータ以外に、PDA (Personal Digital Assitants)、携帯電話機、ゲーム端末機などとすることができる。

【 0 1 3 2 】

一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、ネットワークや記録媒体からインストールされる。

【 0 1 3 3 】

この記録媒体は、図 2 に示すように、装置本体とは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク 4 1 (フロッピディスクを含む)、光ディスク 4 2 (CD-ROM (Compact Disk-Read Only

Memory), DVD(Digital Versatile Disk)を含む)、光磁気ディスク 4 3 (MD (Mini-Disk) を含む)、もしくは半導体メモリ 4 4 などよりなるパッケージメディアにより構成されるだけでなく、装置本体に予め組み込まれた状態でユーザに提供される、プログラムが記録されているROM 2 2 や、記憶部 2 8 に含まれるハードディスクなどで構成される。

【0 1 3 4】

なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0 1 3 5】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【0 1 3 6】

【発明の効果】

以上の如く、本発明の情報処理装置および方法、プログラム格納媒体、並びにプログラムによれば、暗号化されたデータとライセンスを識別する識別情報を、所定のフォーマットにフォーマット化して、出力するようにしたので、データが不正に利用されるのを抑制することが可能となる。

【図面の簡単な説明】

【図 1】

本発明を適用したコンテンツ提供システムの構成を示すブロック図である。

【図 2】

図 1 のクライアントの構成を示すブロック図である。

【図 3】

図 1 のクライアントのコンテンツのダウンロード処理を説明するフローチャートである。

【図 4】

図 1 のコンテンツサーバのコンテンツ提供処理を説明するフローチャートであ

る。

【図 5】

図 4 のステップ S 2 6 におけるフォーマットの例を示す図である。

【図 6】

図 1 のクライアントのコンテンツ再生処理を説明するフローチャートである。

【図 7】

図 6 のステップ S 4 3 のライセンス取得処理の詳細を説明するフローチャートである。

【図 8】

図 6 のステップ S 4 5 におけるライセンス更新処理の詳細を説明するフローチャートである。

【図 9】

図 1 のライセンスサーバのライセンス付与の処理を説明するフローチャートである。

【図 1 0】

ライセンスサーバのライセンス付与処理を説明する図である。

【図 1 1】

図 1 のクライアントのコンテンツのコピー処理を説明するフローチャートである。

【図 1 2】

図 1 のクライアントのコンテンツのコピーによる利用を説明する図である。

【図 1 3】

図 1 のクライアントのコンテンツのコピーによる利用を説明する図である。

【図 1 4】

ライセンスとコンテンツの関係を説明する図である。

【図 1 5】

キーの構成を説明する図である。

【図 1 6】

キーの構成とライセンスの関係を説明する図である。

【図 1 7】

図 5 の EKB の例を示す図である。

【符号の説明】

1 - 1, 1 - 2 クライアント, 2 インターネット, 3 コンテンツサーバ,
4 ライセンスサーバ, 5 課金サーバ, 2 0 タイマ, 2 1
CPU, 2 4 暗号化復号部, 2 5 コーデック部, 2 6 入力部, 2 7
出力部, 2 8 記憶部, 2 9 通信部

【書類名】 図面

【図1】

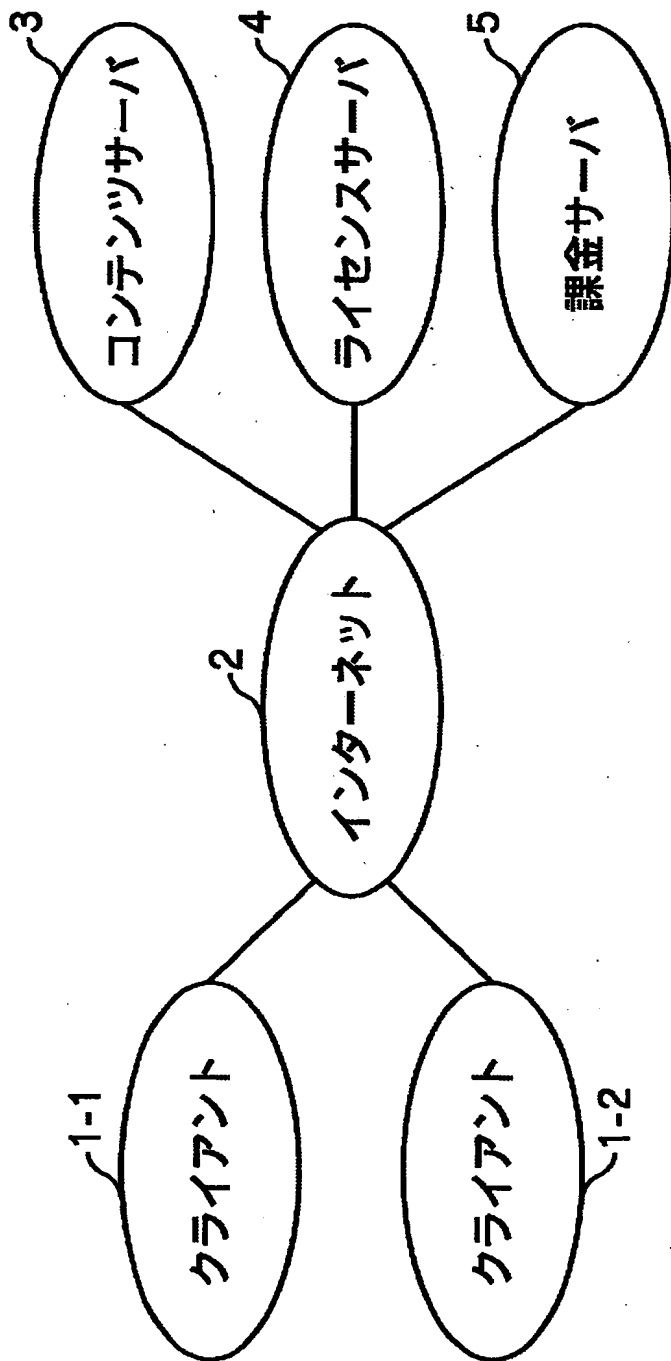
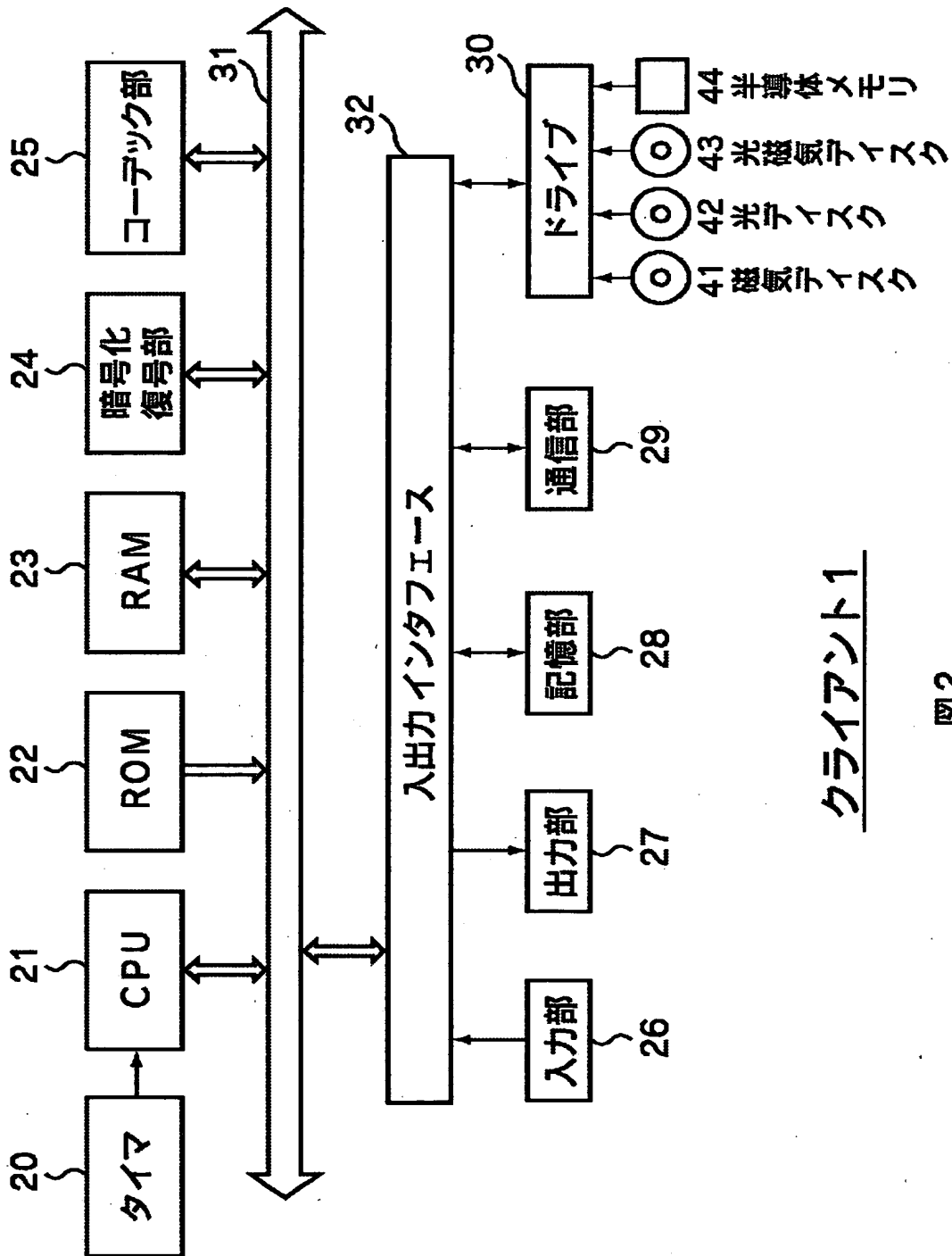


図1

【図2】



クライアント1

図2

【図3】

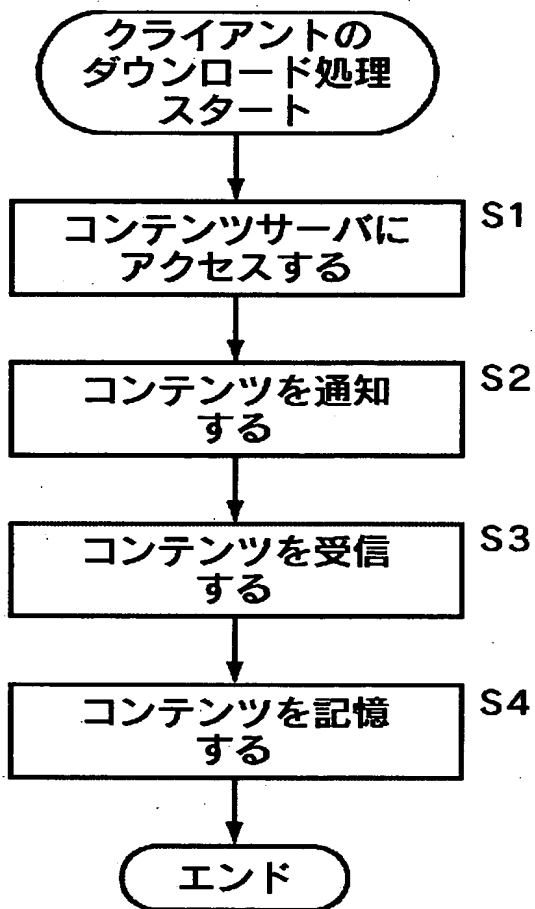


図3

【図 4】

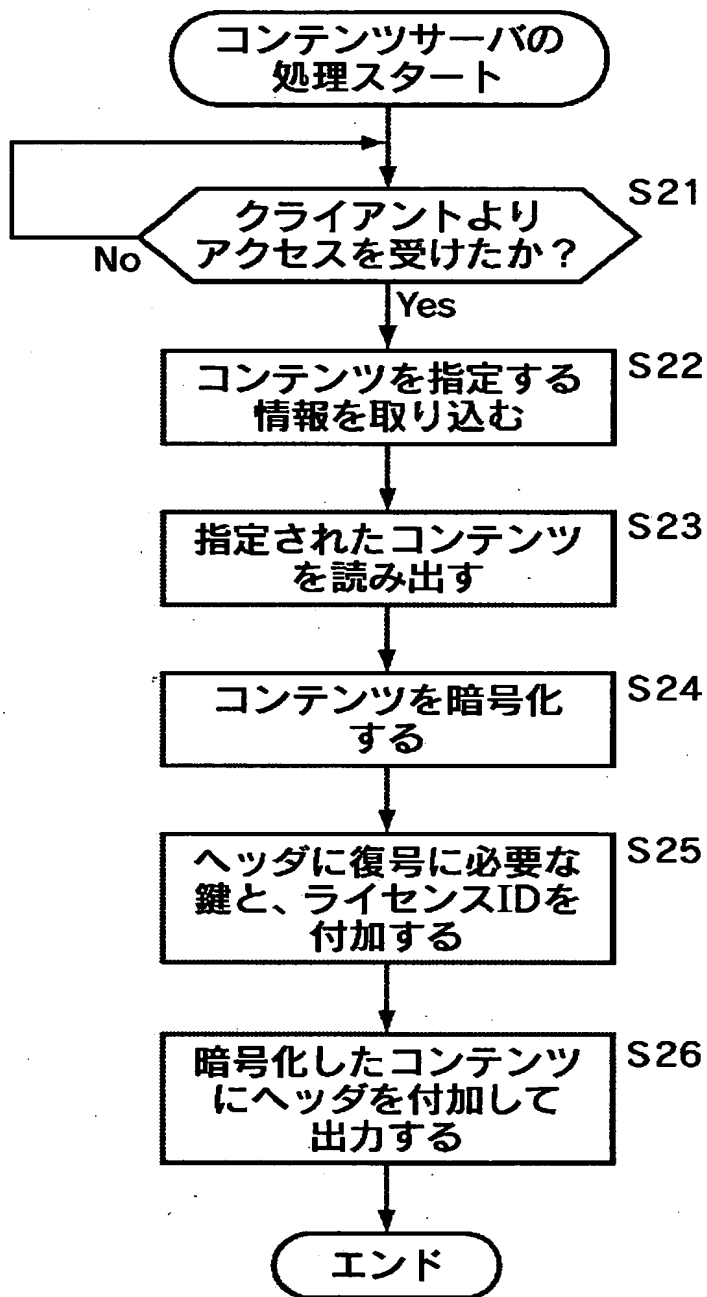


図 4

【図 5】

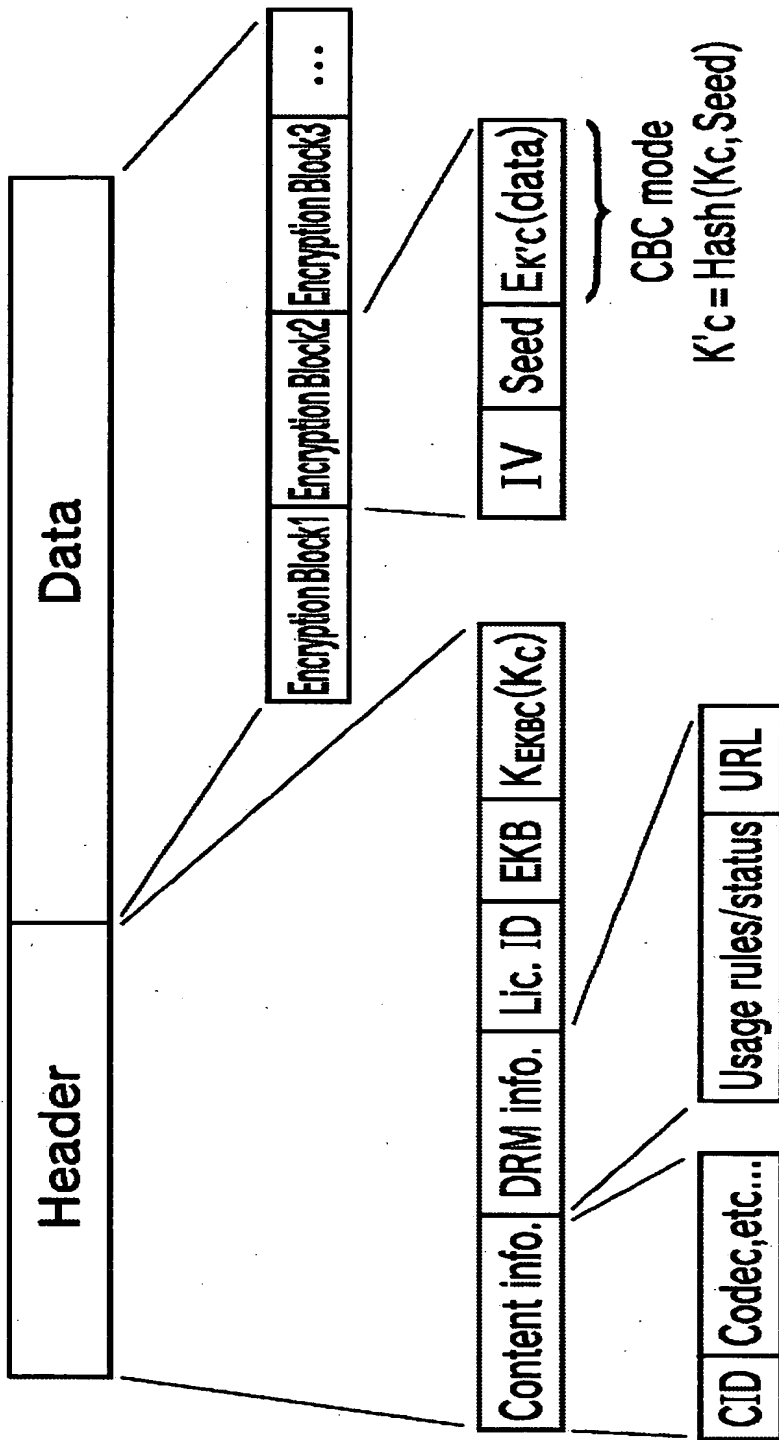


図 5

【図 6】

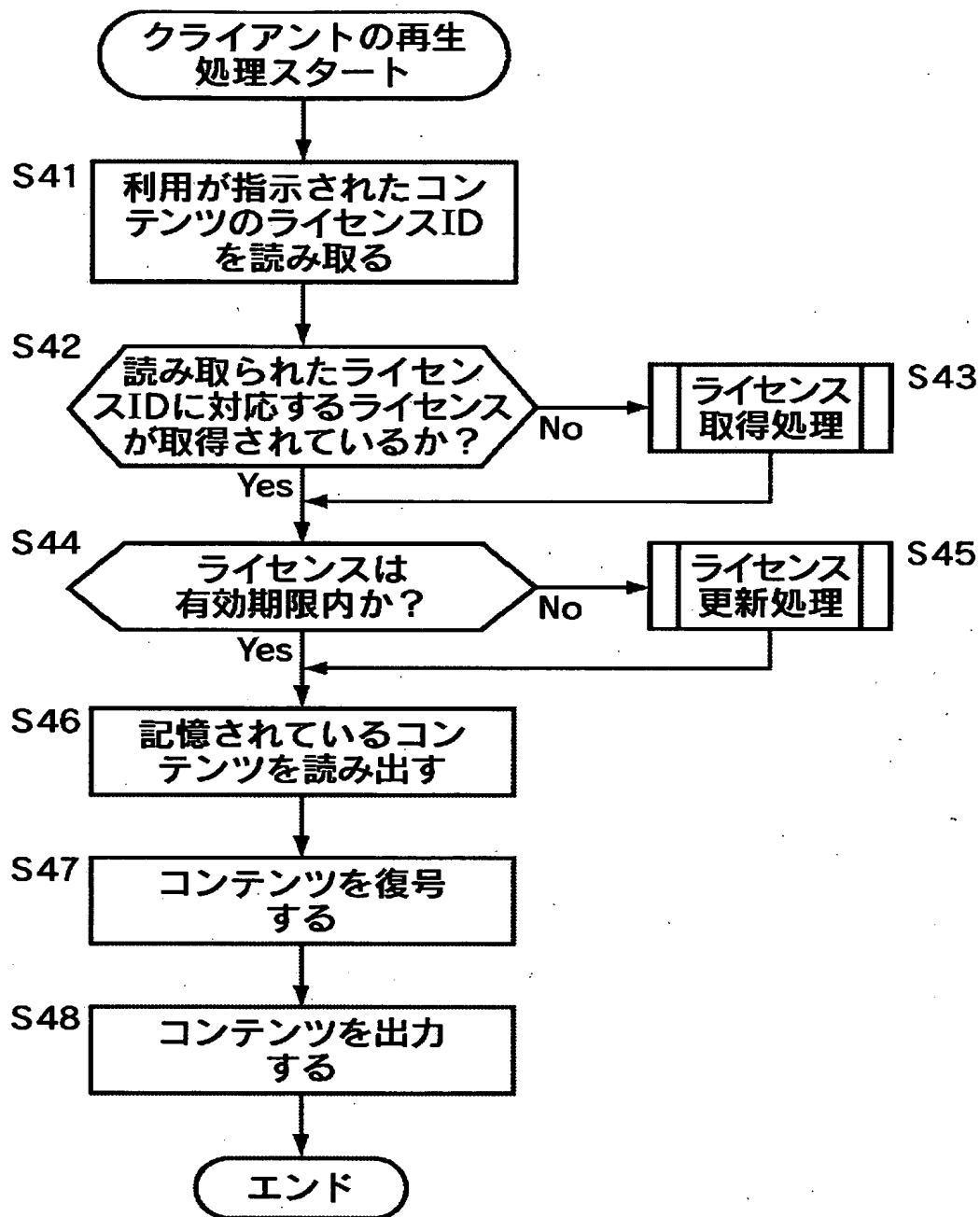


図 6

【図 7】

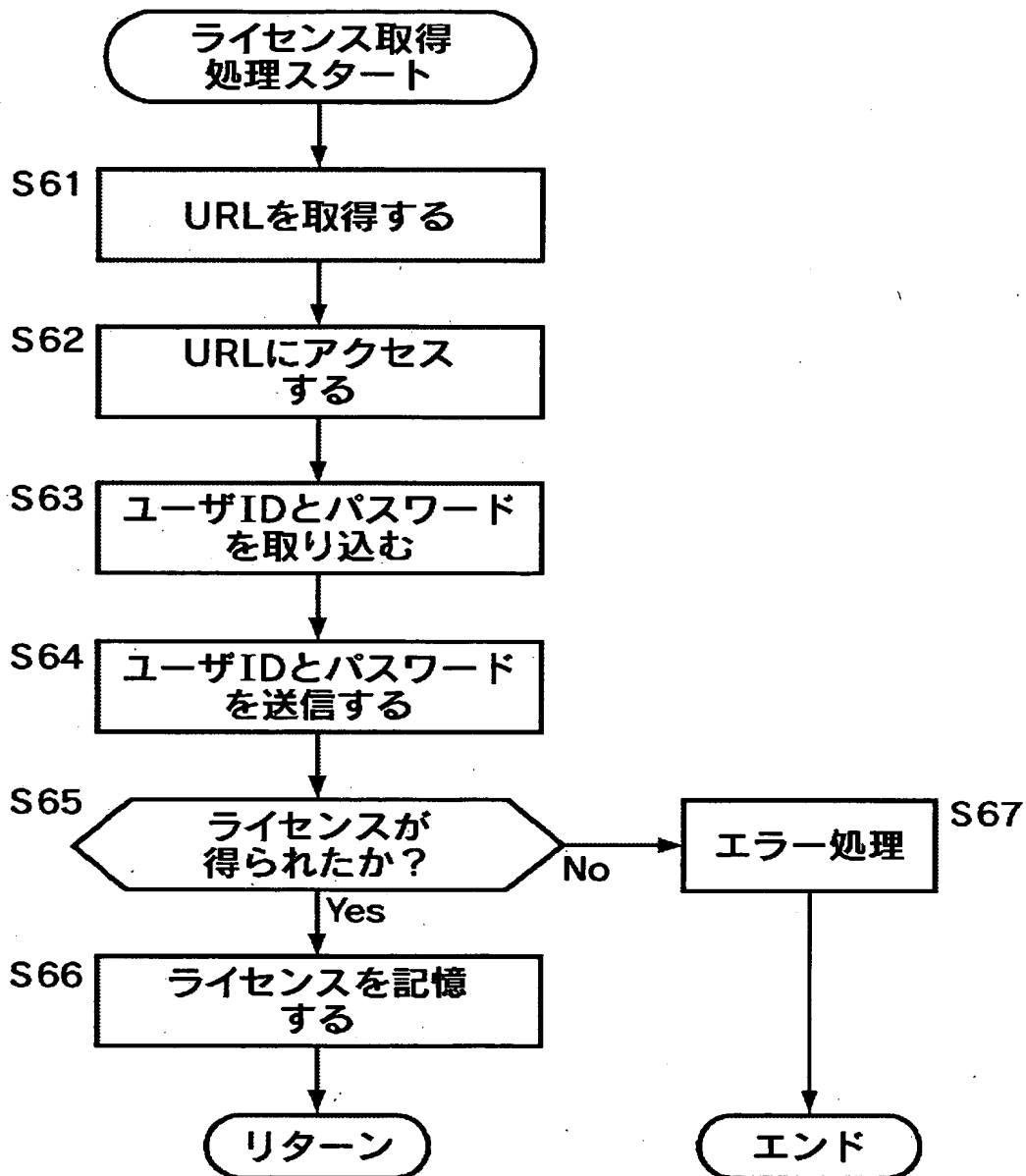


図 7

【図8】

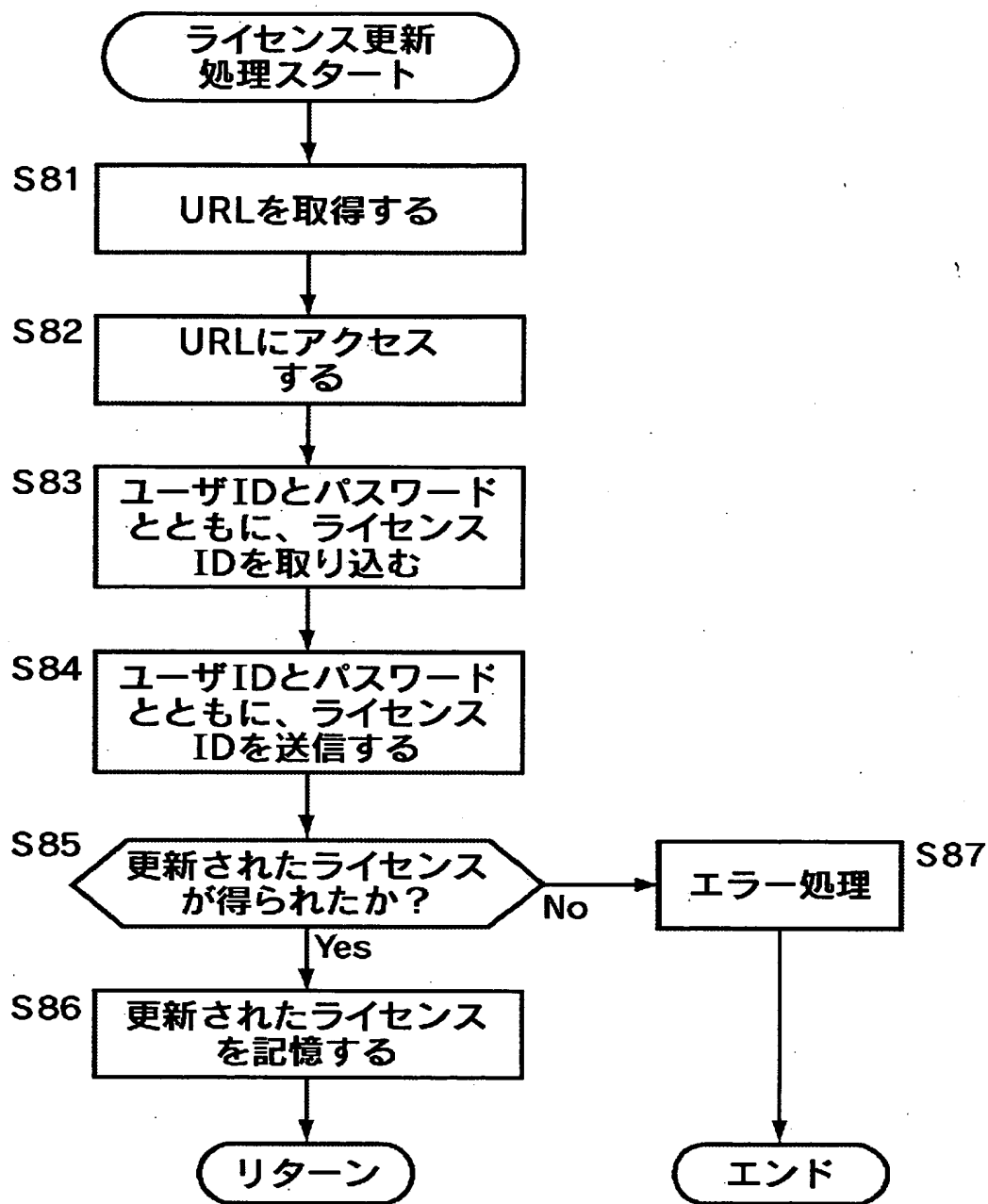


図8

【図9】

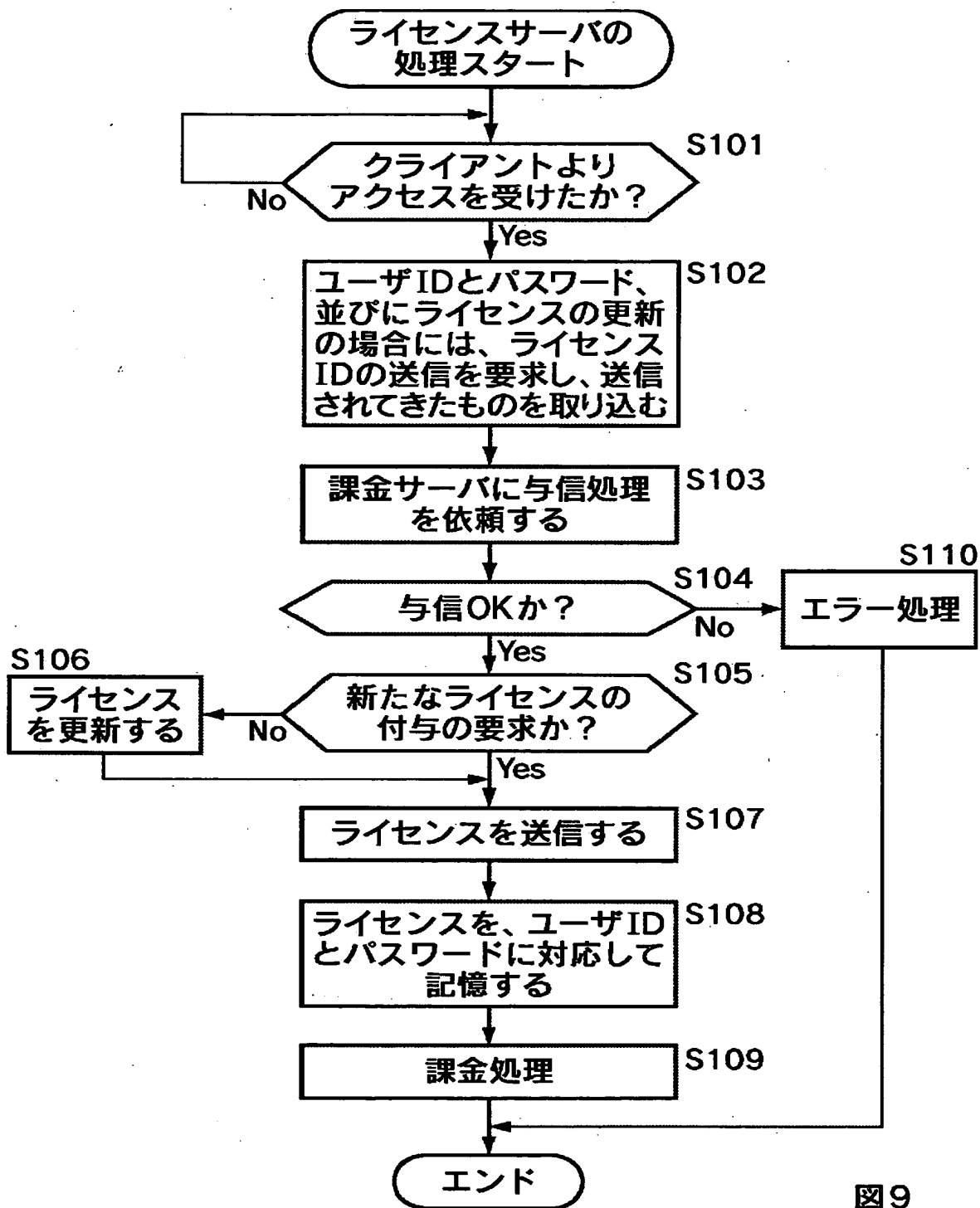


図9

【図10】

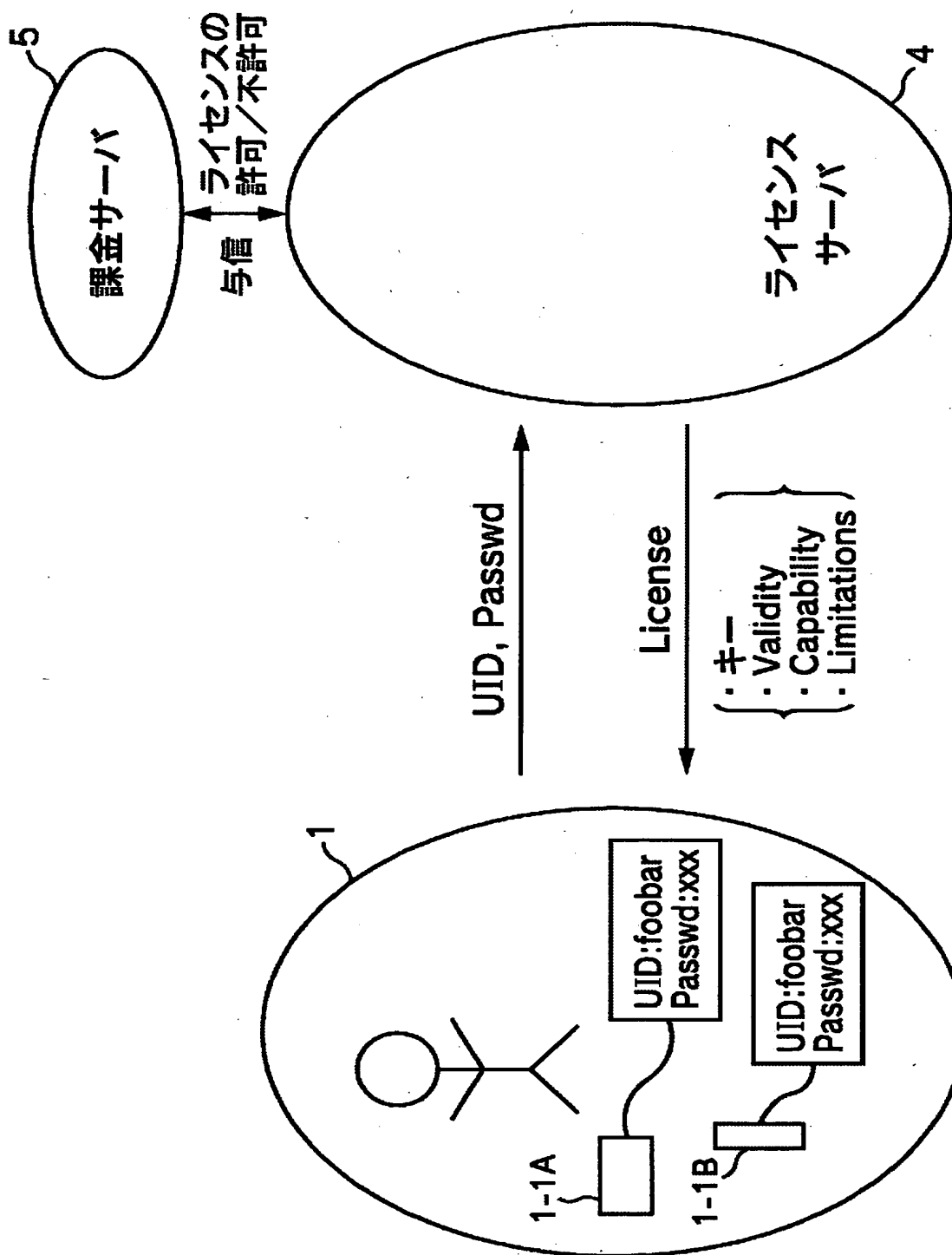


図10

【図11】

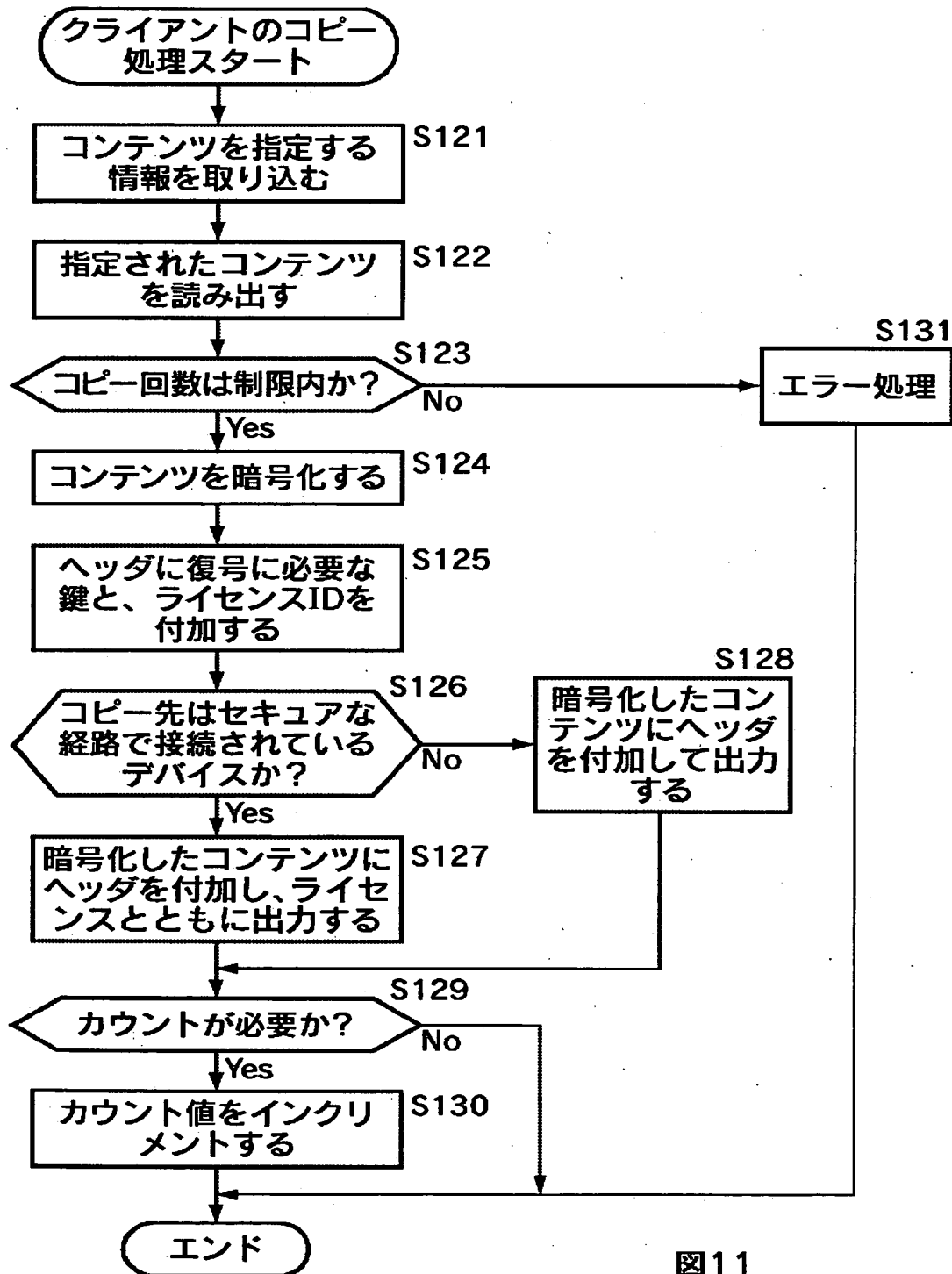
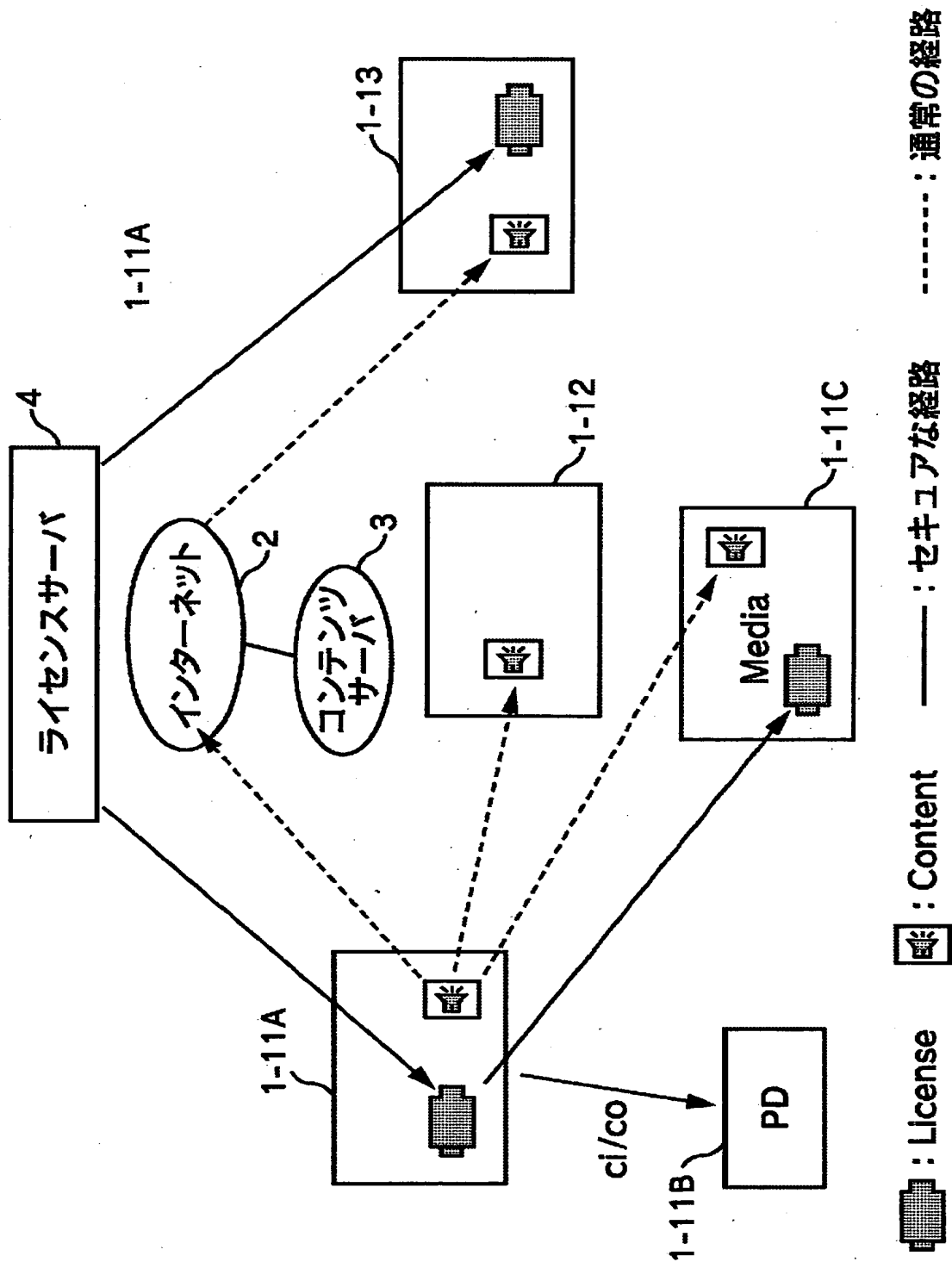


図11

【図 12】



12

【図 13】

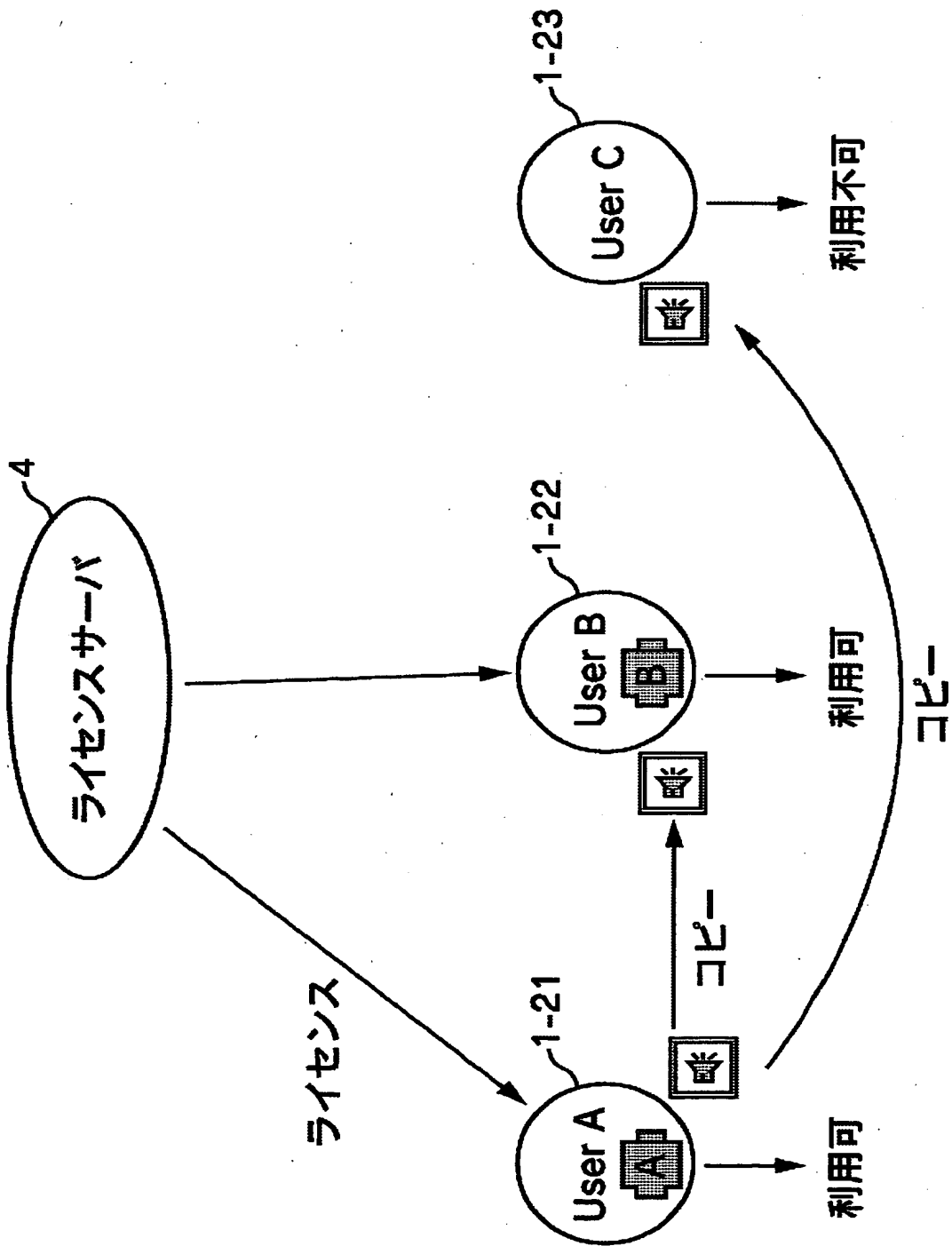


図13

【図 14】

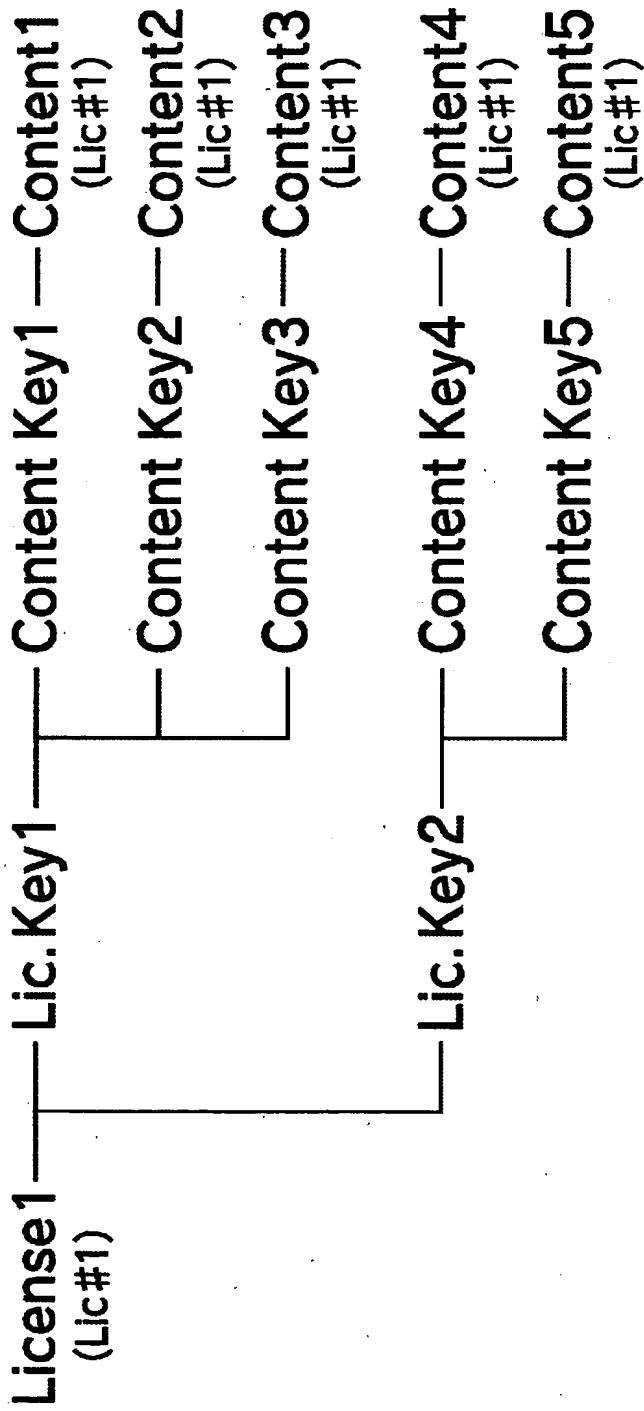


図14

【図 1 5】

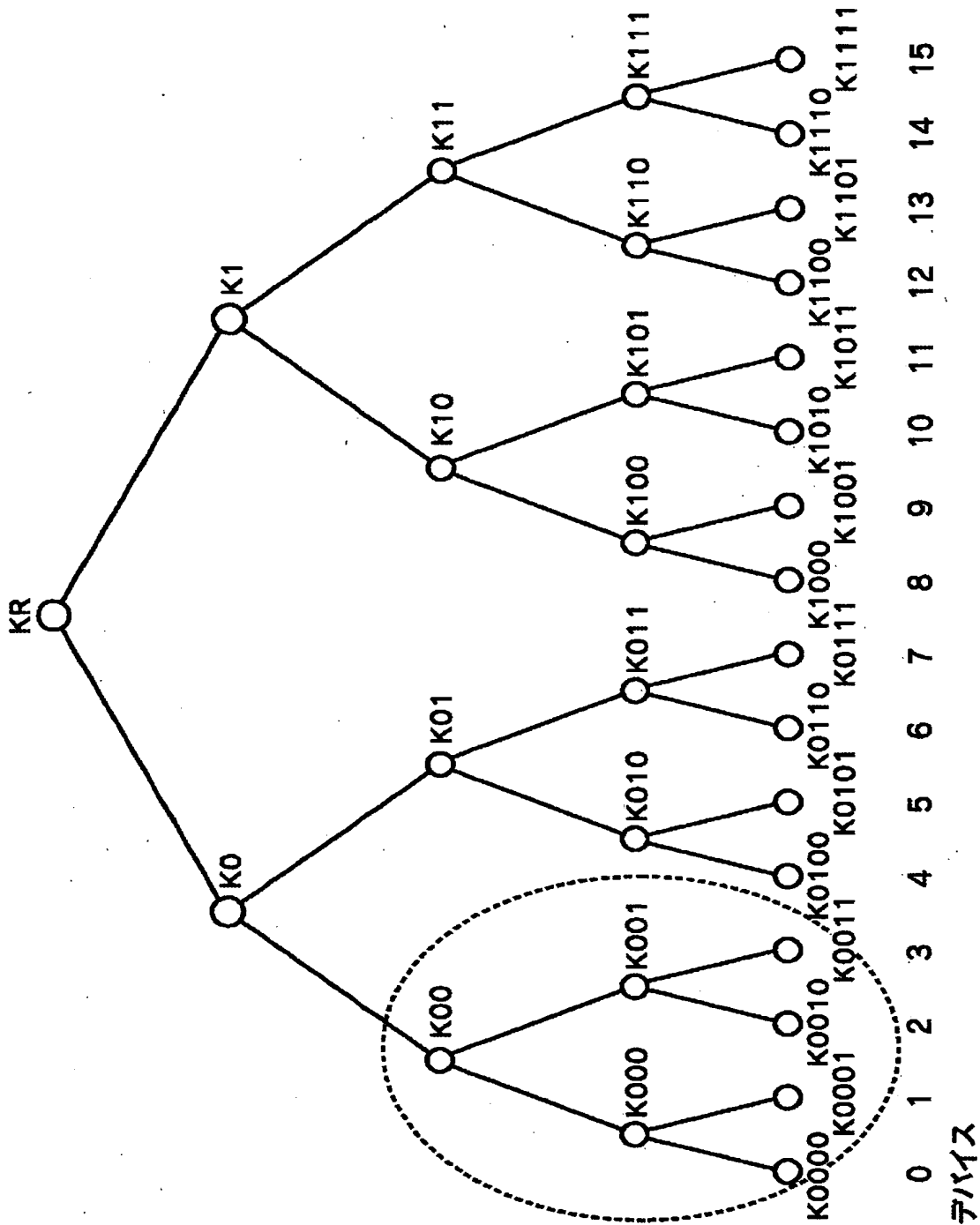


図15

【図16】

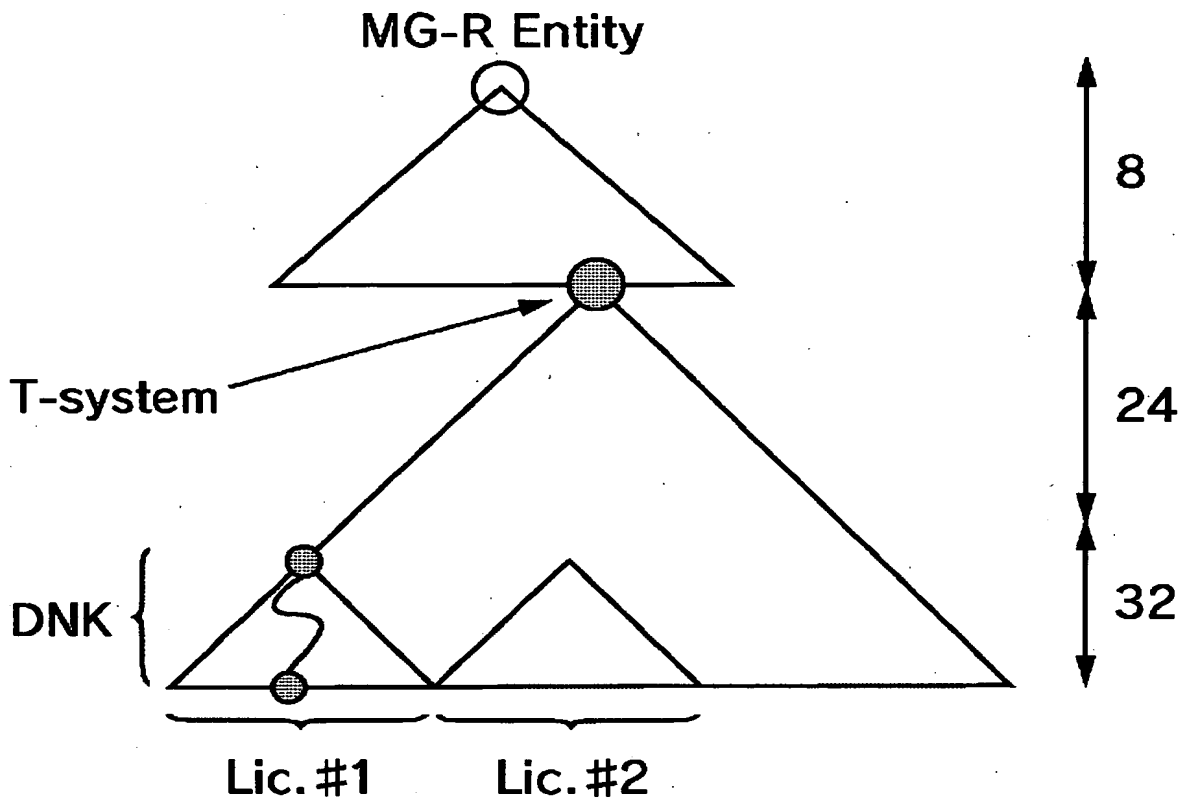


図16

【図17】

EKB
Kdnk (Lic.Key1)

図17

【書類名】 要約書

【要約】

【課題】 コンテンツが不正にコピーされ、利用されるのを防止する。

【解決手段】 コンテンツサーバは、クライアントにインターネットを介してコンテンツを提供するとき、コンテンツを暗号化する。その暗号化されたコンテンツのヘッダには、そのコンテンツを利用するとき必要とされるライセンスを識別するライセンスIDが記述される。クライアントは、ライセンスIDに対応するライセンスをライセンスサーバにアクセスして取得することで、暗号化されたコンテンツを復号するのに必要なキーを含むライセンスを取得する。

【選択図】 図5

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日
[変更理由] 新規登録
住 所 東京都品川区北品川6丁目7番35号
氏 名 ソニー株式会社